Updating the NSX or Director System

If you are updating an NSX or Director system, you must do the following before proceeding with the installation:

1. **Shut down the NetRanger daemons using the** `nrstop` **command.**
2. **Shut down OpenView by bringing down all open user interfaces using the** Map→Exit **menu item. Then type** `ovstop` **to complete the shut down.**
3. **Make a backup copy of the entire /usr/nr directory.**
4. **Uninstall the Director software. If you are uninstalling from an HP-UX system, please refer to Appendix F, *Uninstalling the Director*, page F-1, steps 5–8. If you are uninstalling from a Sun Solaris system, please refer to page F-3, steps 5–8.** This step preserves the former configuration.

You can now proceed with the installation.

Installing HP-UX 10.10 or greater

Follow the directions in your HP-UX documentation to either install or upgrade to HP-UX 10.10.

Installing HP OpenView 4.1 or greater

HP OpenView will not install correctly if TCP/IP is not functioning properly. The following parameters must be set before you install HP OpenView:

- IP Address
- Hostname
- Subnet mask
- Default gateway hostname
- Default gateway IP address
- System time and timezone

1. **To set these parameters, log on as user root, and then you can either run the command**

   /etc/set_parms initial

   or follow these steps:

   a) **From the Toolboxes subpanel on the Common Desktop Environment (CDE) Front Panel, choose** General→System_Admin→Set Networking

      Enter the appropriate IP information. Although you will be asked about DNS and NIS configurations, you should choose **Cancel** for these options unless you are *certain* you know the proper IP addresses for these services.

   CAUTION

   If an incorrect IP address is entered for these services, the machine may not reboot properly.

   b) **Configure the proper hostname using the following command:**

   ```
   /etc/set_parms hostname
   ```

   CAUTION

   Do not try to change the hostname by editing /etc/hosts. This will cause the CDE to fail.

   c) **Set the machine's time zone using the following command:**

   ```
   /etc/set_parms timezone
   ```

2. **Reboot the machine. Once the machine has rebooted, you should be able to ping your loopback address (**`ping 127.0.0.1`**), ping your IP address (**`ping <IPAddress>`**), resolve your loopback address (**`nslookup 127.0.0.1`**), resolve your IP address (**`nslookup <IPAddress>`**), and resolve your hostname (**`nslookup <hostname>`**). Also, the timezone should be correct (**`date`**). Do not go to the next step until these TCP/IP parameters are properly configured.**

3. **Install HP OpenView 4.1 or greater on the HP-UX system (see the HP OpenView Installation Manual for details).**

4. **Add the following lines to the /.profile for user root. Please note the space between the "." and the "/":**

   ```
   . /opt/OV/bin/ov.envvars.sh
   export PATH=$PATH:$OV_BIN
   ```

   NOTE

   If user root does not use korn or bourne shell, then you must translate and place these lines in the appropriate shell configuration file.

Director Installation for HP-UX systems

To install the NetRanger Director software, follow these steps:

1. **Using** su, **log on as user root.**
2. **To load the OpenView environment variables, type the following command:**

   ```
   . /opt/OV/bin/ov.envvars.sh
   ```

3. **If the OpenView user interface is running, stop it now by selecting** Map→Exit **from the OpenView menu. If other users have other copies of the user interface running and exported to other displays, ask them to shut down the user interface temporarily.**
4. **Put the NetRanger/Director tape in the tape drive if you have not already done so.**
5. **Go to the /tmp directory by typing**

   ```
   cd /tmp
   ```

6. **The NetRanger/Director install tape should contain compressed .tar files whose names have the following format:**

   ```
   WGCnsx.<version>.<release>.<mod level>.<sys type>.tar.Z

   WGCdrctr.<version>.<release>.<mod level>.<sys type>.tar.Z

   WGCcfgs.<version>.<release>.<mod level>.<sys type>.tar.Z

   WGCsapd.<version>.<release>.<mod level>.<sys type>.tar.Z

   JDK_<version>_<release>_<mod level>-<sys type>.tar.Z
   ```

7. **Untar each of the .tar files from the tape using the following syntax (you must run this command for each of the five files):**

   ```
   tar -xvf /dev/rmt/0m <filename>
   ```

   Where <filename> is the name of the compressed tar file.

8. **Uncompress these files using the following syntax (you must run this command for each of the five files):**

   ```
   uncompress <filename>
   ```

   Once the files are uncompressed, they should no longer have the ".Z" extension.

9. **Untar the uncompressed files, *except for the Java Development Kit*, using the following syntax:**

   ```
   tar -xvf <filename>
   ```

10. **Untar the Java Development Kit using the following commands:**

    ```
    mkdir -p /opt/SUNWjava

    cd /opt/SUNWjava

    tar -xvf /tmp/JDK_1_0_1-hpux10.tar

    mv JDK-1.0.1 JDK
    ```

11. **Run the install software by typing the following commands for each component:**

    Installing the NSX Interface software

    ```
    /usr/sbin/swinstall -v -x mount_all_filesystems=false -s /tmp/WGCnsx WGCnsx
    ```

    Installing the DBMS software

    ```
    /usr/sbin/swinstall -v -x mount_all_filesystems=false -s /tmp/WGCsapd WGCsapd
    ```

    Installing the Network Management Interface software

    ```
    /usr/sbin/swinstall -v -x mount_all_filesystems=false -s /tmp/WGCdrctr WGCdrctr
    ```

    Installing the Remote Configuration software

    ```
    /usr/sbin/swinstall -v -x mount_all_filesystems=false -s /tmp/WGCcfgs WGCcfgs
    ```

12. **The Director installation process creates an account for the user "netrangr". You must set a password for that user. To set the password, type**

    ```
    passwd netrangr
    ```

13. **If** */usr/nr/tmp* **and** */usr/nr/var* **do not already exist, type the following command to create them:**

    ```
    mkdir /usr/nr/tmp

    mkdir /usr/nr/var
    ```

14. **If you would like the NetRanger daemons to start automatically at boot time, type:**

    ```
    /usr/nr/bin/install add
    ```

15. **Examine the file** */tmp/nrdirmap.install.out* **to ensure that no errors occurred.**

The installation is now complete. Go to the section entitled *Post-Installation for HP-UX and Sun Solaris Systems.*

Pre-Installation for Sun Solaris Systems

Before you begin the installation process, verify that you meet the Software and Hardware Requirements listed below.

Software Requirements

You must have the following software either installed on your Sun workstation or you must have the following software media and instructions:

- Solaris 2.4 or greater
- HP OpenView 4.1 or greater

If you are installing the NetRanger/Director on a Sun workstation that already has Solaris 2.4 or greater *and* HP OpenView 4.1 or greater installed, you can go to the section in this chapter entitled *Director Installation for Sun Solaris Systems.*

The disk space requirements for the Director software are dictated by the amount of space needed for HP OpenView, the amount of space needed for NetRanger logging and database staging, and the amount of space needed for the NetRanger executables and configuration files. NetRanger logging and database staging requires anywhere from 250 MB to 1 GB in /usr/nr/var, depending on the amount of network traffic, type of logging, etc.

Hardware Requirements

The hardware requirements for the NetRanger/Director are dictated by the Hardware requirements of HP OpenView. Consult the HP OpenView Installation documentation to ensure that your machine is powerful enough to run HP OpenView. In general, it is recommended that you use a dedicated machine that has at least 64 MB of RAM and at least 2 GB of disk space.

Updating the NSX or Director System

If you are updating an NSX or Director system, you must do the following before proceeding with the installation:

1. **Shut down the NetRanger daemons using the `nrstop` command.**
2. **Shut down OpenView by bringing down all open user interfaces using the** Map→Exit **menu item. Then type `ovstop` to complete the shut down.**
3. **Make a backup copy of the entire /usr/nr directory.**
4. **Uninstall the Director software. If you are uninstalling from an HP-UX system, please refer to Appendix F, *Uninstalling the Director*, page F-1, steps 5–8. If you are uninstalling from a Sun Solaris system, please refer to page F-3, steps 5–8.** This step preserves the former configuration.

You can now proceed with the installation.

Installing Solaris 2.4 or greater

Follow the directions in your Sun Solaris documentation to either install or upgrade to Solaris 2.4.

Installing HP OpenView 4.1 or greater on Solaris 2.4 or greater

1. **Before attempting to install HP OpenView, ensure that the following parameters are set correctly:**

- IP Address
- Hostname
- Subnet mask
- Default gateway IP Address
- Default gateway Hostname
- System time and timezone

2. **Reboot the machine. Once the machine has rebooted, you should be able to ping your loopback address (`ping 127.0.0.1`), ping your IP address (`ping <IPAddress>`), resolve your loopback address (`nslookup 127.0.0.1`), resolve your IP address (`nslookup <IPAddress>`), and resolve your hostname (`nslookup <hostname>`). Also, the timezone should be correct (`date`). Do not go to the next step until these TCP/IP parameters are properly configured.**

CAUTION
HP OpenView will not install correctly if TCP/IP is improperly configured.

3. **Install HP OpenView 4.1 or greater on the Sun Solaris machine (see the HP OpenView Installation Manual for details).**

CAUTION
• The HP OpenView installation will fail if semaphores are not enabled. Please refer to the section entitled Requirements for SunOS and Solaris Systems in the *HP OpenView Network Node Manager Products Installation Guide* to enable semaphores. • HP OpenView 4.1.0 will not install on Solaris 2.5.x without an OpenView patch. Please contact your authorized HP representative to obtain this patch. (HP OpenView 4.1.1 and greater do not require this patch.)

5. **Add the following lines to the /.profile for user root. Please note the space between the "." and the "/":**

   ```
   . /opt/OV/bin/ov.envvars.sh
   export PATH=$PATH:$OV_BIN
   ```

Director Installation for Sun Solaris Systems

To install the NetRanger Director software on a Sun Solaris platform, follow these steps:

1. **Using** `su`**, log on as user root.**
2. **To load the OpenView environment variables, type the following command:**

   ```
   . /opt/OV/bin/ov.envvars.sh
   ```

3. **If the OpenView user interface is running, stop it now by choosing** Map→Exit **from the OpenView menu. If other users have other copies of the user interface running and exported to other displays, ask them to shut down the user interface temporarily.**
4. **Put the NetRanger/Director tape in the tape drive if you have not already done so.**
5. **Go to the /tmp subdirectory by typing the following command:**

   ```
   cd /tmp
   ```

6. **The NetRanger/Director install tape should contain compressed .tar files whose names have the following format:**

   ```
   WGCnsx.<version>.<release>.<mod level>.<sys type>.tar.Z

   WGCdrctr.<version>.<release>.<mod level>.<sys type>.tar.Z

   WGCcfgs.<version>.<release>.<mod level>.<sys type>.tar.Z

   WGCsapd.<version>.<release>.<mod level>.<sys type>.tar.Z

   JDK-<version>_<release>_<mod level>-<sys type>.tar.Z
   ```

7. **Untar each of the .tar files from the tape using the following syntax (you must run this command for each of the five files):**

   ```
   tar -xvf /dev/rmt/0m <filename>
   ```

   Where `<filename>` is the name of the compressed tar file.

8. **Uncompress these files using the following syntax (you must run this command for each of the five files):**

   ```
   uncompress <filename>
   ```

   Once the files are uncompressed, they should no longer have the ".Z" extension.

9. **Untar the uncompressed files, *except for the Java Development Kit*, using the following syntax:**

   ```
   tar -xvf <filename>
   ```

10. **Untar the Java Development Kit using the following commands:**

    ```
    mkdir -p /opt/SUNWjava

    cd /opt/SUNWjava

    tar -xvf /tmp/JDK-1_0_2-solaris2-sparc.tar

    mv java JDK

    cd /tmp
    ```

11. **Run the "package add" program by typing:**

    ```
    pkgadd -d .
    ```

12. **Select the "WGCnsx" product from the "available packages" list.**
13. **Answer "yes" to the question about "install suid programs".**
14. **Answer "yes" to run the script as root.**
15. **Once the WGCnsx installation process has completed, select the "WGCdrctr" product from the "available packages" list.**
16. **Answer "yes" to any other questions the installation process might ask.**
17. **Select the "WGCcfg" product from the "available packages" list.**
18. **Answer "yes" to any other questions the installation process might ask.**
19. **Select the "WGCsapd" product from the "available packages" list.**
20. **Answer "yes" to any questions the installation process might ask.**
21. **After the installation procedure is complete, type "q" to quit.**
22. **The Director installation process creates an account for the user "netrangr". You must set a password for that user. To set the password, type**

    ```
    passwd netrangr
    ```

23. **If *[/usr/nr/tmp]* and *[/usr/nr/var]* do not already exist, type the following to create them:**

    ```
    mkdir /usr/nr/tmp

    mkdir /usr/nr/var
    ```

24. **If you would like the NetRanger daemons to start automatically at boot time, type:**

    ```
    /usr/nr/bin/install add
    ```

25. If this is a Solaris 2.4 installation, run the script below. If this is not a Solaris 2.4 installation, you do not need to run this script.

```
/usr/nr/bin/postinstall.sh
```

26. Examine the file */tmp/nrdirmap.install.out* **to ensure that no errors occurred.**

The installation is now complete.

Post-Installation for HP-UX *and* Sun Solaris Systems—Cleanup

1. **As user root, start the HP OpenView daemons by typing the following:**

   ```
   $OV_BIN/ovstart
   ```

   If the ovstart executable is not found, then the `$OV_BIN` environment variable is probably not set properly in root's .profile. To set the variable, please refer to the step on loading the OpenView environment.

2. **To ensure that all OpenView daemons are running properly, type the following command:**

   ```
   $OV_BIN/ovstatus
   ```

3. **Remove all NetRanger Director .tar files from the /tmp directory using the** `rm` **command.**

4. **From /tmp, remove the WGC directories by typing the following:**

   ```
   rm -rf WGC*.*
   ```

OPTIONAL

There is an OpenView daemon called *netmon* whose function is network mapping and availability monitoring. This daemon can be CPU-intensive. If you are only using OpenView to run the NetRanger Director, then it is not necessary to run this daemon.

To disable the *netmon* daemon, run the following commands:

```
$OV_BIN/ovstop netmon

$OV_BIN/ovdelobj $OV_LRF/netmon.lrf
```

5. **If necessary, set the DISPLAY variable in the appropriate** `.profile` **files.**

Post-Installation for HP-UX *and* Sun Solaris Systems—Background Process Configuration Files

The NetRanger background process configuration files enable the Director to communicate with NSX machines on your network. Run the nrconfig utility to configure these files. (Please refer to the *NetRanger Configuration Instructions and Worksheets* for information about the nrconfig utility.)

1. **Before running nrconfig, it is a good idea to stop the OpenView user interface (using the** Map→Exit **menu item), log in as user root, and stop the OpenView daemons by typing**

   ```
   $OV_BIN/ovstop
   ```

2. **Stop the NetRanger/Director daemons by typing (as user netrangr)**

   ```
   /usr/nr/bin/nrstop
   ```

3. **Refer to the *NetRanger Configuration Instructions and Worksheets* and run (as user netrangr)**

   ```
   /usr/nr/bin/nrconfig
   ```

4. **After running nrconfig, verify the following in the files in /usr/nr/etc on the Director machine:**

   - **Verify that the *usr/nr/etc/auths* file lists the Director machine.**
   - **Verify that the */usr/nr/etc/hosts* file contains all of the */usr/nr/etc/hosts* files on the NSX machines. The only difference should be that the *localhost* entry in the Director's file should match the Director's *hostid/orgid* pair.**
   - **Verify that the */usr/nr/etc/organizations* file matches the */usr/nr/etc/organizations* files on the NSX machines.**
   - **Verify that the */usr/nr/etc/*destinations file lists all of the NSX machines that are sending data to the Director machine.**
   - **Verify that the */usr/nr/etc/routes* file contains all of the routes files on the NSX machines.**
   - **Verify that the */usr/nr/etc/*daemons file has listings for *nr.smid, nr.postofficed, nr.configd, and nr.loggerd.* If you are using *sapd* to propagate a relational database, then ensure there is a listing for *nr.sapd.* If you configured *eventd*, then ensure there is a listing for *nr.eventd.* If there is an entry for *nr.sensord* in this file, ensure that it is commented out. (Use the # key to comment out a line.)**
   - **Verify that the */usr/nr/etc/smid.conf* file lists the *loggerd* daemon as a *dupDestination.* (This step is optional.)**
   - **Verify that the */usr/nr/etc/services* and */usr/nr/etc/signatures* files exist.**

5. **After you have installed the NSX machine(s) that will communicate with a particular Director machine, verify the following information in the files in /usr/nr/etc for each NSX machine (this will also need to be done for any subsequent NSX machine installations):**

   - **Verify that the *\/usr/nr/etc/destinations* file is configured to send alarms to the *smld* process on the Director. This is very important. *The Director will not receive alarms if this is not done.***
   - **Verify that the proper name and address of the Director is in the *\/usr/nr/etc/routes* file.**

The installation should now be complete.

Post-Installation for HP-UX *and* Sun Solaris Systems—Configuring the User Interface

The following steps only need to be done once.

1. **Log on as user root.**
2. **Start the OpenView daemons using** `ovstart`.
3. **Log on as user netrangr.**
4. **Start the NetRanger daemons using** `nrstart`.
5. **Start the user interface by typing** `$OV_BIN/ovw &`.
6. **Double-click the** NetRanger **icon.**
7. **Choose the menu option** Map→Maps→Describe/Modify.
8. **Under the** Compound Status **heading, press the** Propagate Most Critical **button.**
9. **Choose** OK.
10. **Choose the menu option** Map→Submaps→Set This Submap As Home.
11. **Choose the menu option** Map→Submaps→Describe/Modify.
12. **Under the** Background Graphics: **heading, press the** Browse... **button.**
13. **From the pop-up list, select the background graphic of your choice. (The usastates.gif is a popular choice). You could also create a custom GIF file with any graphics program and use that GIF file as an OpenView submap background.**
14. **Choose** OK, **and then choose** OK **again.**

The following steps should be done every time a new NetRanger/NSX machine is added to your system:

1. **Run nrconfig to update the configuration files.**
2. **Add the NSX icon to the OpenView map using the following steps:**
   - **Select the** Edit→Add Object **menu function.**
   - **Click on the** Net Device **icon. Several icons will appear in the bottom of the window.**
   - **Drag the** NSX 2000 **icon to the NetRanger submap (the submap containing the Director icon) by pressing and holding the middle mouse button while positioning the mouse pointer over the** NSX 2000 **icon. An** Add Object **window should appear.**

3. **Choose** NetRanger/Director **from the list, and press the** Set Object Attributes **button.**
4. **In the** hostname **field, enter the name of the NSX machine exactly as you entered it in the** ***/usr/nr/etc/hosts*** **file.**
5. **Press the** Verify **button. If you entered the hostname correctly, the Organization and Host Ids should have been filled in for you.**
6. **Once the** hostname, Organization ID, **and** Host ID **are correct, choose** OK.
7. **Press the** Set Selection Name **button. Choose the selection name from the list and then press OK in the Selection Name window. Press the** OK **button in the Add Object Window.**
8. **You should see the** NSX **icon turn green. If you double-click on the NSX icon, you should see icons that represent the processes running on that machine.**

Post-Installation for HP-UX and Sun Solaris Systems—Configuring New Users

By default, only user netrangr is configured to use and reconfigure the NetRanger Director system. If you want to grant Director software access to another user, you must add the user to the UNIX group netrangr. You must also configure the user's shell environment appropriately. Instructions for both are listed below.

- On HP systems, users can be added to and removed from groups using the sam utility. To do this, choose "Accounts for Users and Groups" then choose "Groups".
- On Sun systems, use the admintool to add users to and remove users from groups.

NOTE

On HP Systems, if a user is in the group "netrangr" (but netrangr is not that user's primary group), then the user must type `newgrp - netrangr` to execute nrdirmap.

Sun users do not have to do this.

Configuring the User Environment

User netrangr uses the “ksh” UNIX shell. The environment settings for user netrangr are kept in the file /usr/nr/.profile. The .profile puts /usr/nr/bin in the $PATH, and then it sets environment variables for OpenView, Java, and Oracle.

1. **To configure users other than “netrangr” to use the Director, ensure that the user uses “ksh” (This can be confirmed by viewing the** `/etc/passwd` **file.) and add the following lines from the /usr/nr/.profile to the user’s $HOME/.profile:**

```
# Begin .profile additions
PATH=/usr/nr/bin:/usr/sbin:/usr/bin:/usr/ucb:/etc
export PATH
if [ -d /opt/OV ] ; then
        . /opt/OV/bin/ov.envvars.sh
        PATH=$OV_BIN:$PATH
        export PATH
        LD_LIBRARY_PATH=$OV_LIB:$LD_LIBRARY_PATH
        export LD_LIBRARY_PATH
fi

if [ -d /opt/SUNWjava ] ; then
        PATH=/opt/SUNWjava/JDK/bin:$PATH
        export PATH
        LD_LIBRARY_PATH=$HOME/lib:$LD_LIBRARY_PATH
        LD_LIBRARY_PATH=/opt/SUNWjava/JDK/lib/$sysType:$LD_LIBRARY_PATH
        export LD_LIBRARY_PATH
        CLASSPATH=$HOME/classes:/opt/SUNWjava/lib
        export CLASSPATH
fi

if [ -d /work/app/oracle ] ; then

        ORACLE_HOME=/work/app/oracle/product/7.3.2
        export ORACLE_HOME
        PATH=$PATH:$ORACLE_HOME/bin
        export PATH
        LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME/lib
        export LD_LIBRARY_PATH
fi

# End .profile additions
```

If the user must use a shell other than "ksh", then the lines above must be translated into the appropriate scripting language and placed in the appropriate shell startup file.

Post-Installation for HP-UX—*eventd* Configuration

If you plan to use the NetRanger *eventd* daemon, you should reconfigure the maximum number of processes that the HP Kernel will allow. Otherwise, if *eventd* receives many alarm notifications in a short time, *eventd*s executed processes could exceed the configured limits.

To reconfigure the Kernel, follow these steps:

1. **As root, type:**

   ```
   sam &
   ```

2. **Choose** Kernel Configuration→Configurable Parameters.
3. **Highlight "nproc", then choose** Actions→Modify Configurable Parameters.
4. **Change the "Formula/Value" to the following:**

   ```
   (250+8*MAXUSERS)
   ```

5. **Press OK.**
6. **Highlight "maxuprc", then choose** Actions→Modify Configurable Parameters.
7. **Change the "Formula/Value" to the following:**

   ```
   300
   ```

8. **Press** OK.
9. **Choose** File→Exit.
10. **Choose** OK **to create the new Kernel and reboot the machine.**

Install and Configure the NetRanger NSX Sensor

Installing the NSX involves the following steps:

- Position the NSX in a stable location
- Attach power, network, and modem cables
- Initial access and NSX system configuration
- NetRanger-specific configuration

Position the NSX

WheelGroup recommends that the NSX be placed physically close to the BorderGuard with which it will be operating. The NSX should be placed on a solid, flat, well-ventilated surface, such as a desk, shelf, equipment rack, or wiring closet. Ideally, the NSX should be placed within a standard communications rack.

Attach Power, Network, and Modem Cables

Proper installation of the NSX requires that the power cable and network cable are connected. The NSX and BorderGuard should also be plugged into an Uninterruptable Power Supply (UPS) to ensure continuous operation during power failures. The NSX is pre-configured to operate using the 10BaseT connector on the Ethernet card. Attachment of a modem cable to the internal modem is optional for most installations. However, this option is required only if initial configuration of the NSX will occur over a dial-up connection.

The NSX operating system is Solaris 2.5 x86. It is pre-installed on the internal hard disk along with the NetRanger software. The power to the NSX should never be turned off without first properly shutting down Solaris. Failure to do so may cause the file system on the NSX to become corrupted with possible loss of data. Repeated power-offs of this kind may cause the NSX to not boot properly or not at all. If this occurs, please contact your NetRanger maintenance provider.

Initial Access and NSX System Configuration

The NSX may be initially configured by logging in through one of the following methods:

- network
- modem
- serial
- console

Network Access

The NSX login prompt may be accessed via the network. When you use this method of access, the login prompt will look similar to the example below. This requires attaching a computer to the same Ethernet LAN as the NSX and then using TELNET to connect to the NSX. The default IP address of the NSX is 10.1.9.201 with a netmask of 255.255.255.0. This means that the computer used to access the NSX must be configured with an IP address between 10.1.9.1 and 10.1.9.254 excluding 10.1.9.201.

```
UNIX(r) System V Release 4.0 (nsx)

login:
```

Modem Access

The NSX login prompt may be accessed via the internal modem. When you use this method of access, the login prompt will look similar to the example below. This requires the installation of a standard telephone cable to the RJ-11 jack labeled TELCO located on the back of the NSX. The modem is configured to answer after the first ring. The NSX is pre-configured for a vt100 terminal once the modem connection is established.

```
modem login:
```

Serial Access

The NSX login prompt may be accessed via a serial connection to the COM1 port. When you use this method of access, the login prompt will look similar to the example below. This requires that a null-modem cable be attached between the NSX and a VT100-compatible terminal or a computer running terminal emulation software. Set the terminal or terminal emulation software to the following specifications:

```
Terminal:  VT100

Baud Rate:  9600

Word Length:  8 bit

Stop Bit: 1 bit

Parity:  None
```

```
ttya login:
```

Console Access

The NSX login prompt may be accessed via the console. When you use this method of access, the login prompt will look similar to the example below. This requires the attachment of a keyboard and monitor to the NSX. A standard VGA-compatible monitor is adequate for access.

```
nsx console login:
```

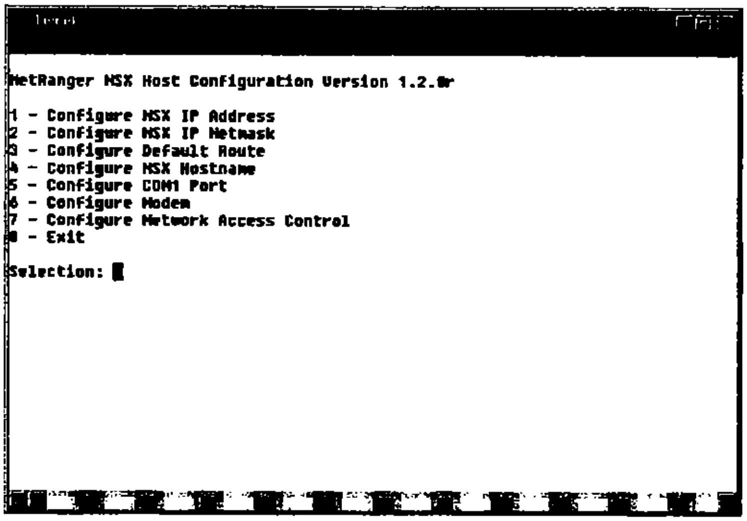
Logging In

Once the prompt is available, login as user *netrangr*. A password is not required, even though you will be prompted to set one. Once the initial prompt is accessed, use the **su** command to become the root user. The default root password is **attack**. Once the root prompt is accessed, immediately change the root password by using the **passwd** command.

NOTE

Write down the new passwords you have chosen for both *netrangr* and *root* and store them in a secure location.

Once you have set the account password, you are ready to configure the machine's basic settings via the **sysconfig-nsx** utility. Note that the utility must be run by user root. The **sysconfig-nsx** command will display a menu, illustrated in Figure III-1 below.



```
NetRanger NSX Host Configuration Version 1.2.0r

1 - Configure NSX IP Address
2 - Configure NSX IP Netmask
3 - Configure Default Route
4 - Configure NSX Hostname
5 - Configure COM1 Port
6 - Configure Modem
7 - Configure Network Access Control
0 - Exit

Selection:
```

Figure III-1:NetRanger NSX Host Configuration Screen

Proper installation of the NSX requires configuration of the IP address, IP netmask, and default route. Be sure to configure the network access control to specify a list of IP addresses that require TELNET access to the NSX. The configuration utility only modifies the startup files for the operating system. The NSX will have to be rebooted for the new changes to take effect. Once configuration is complete, enter the command `init 6` to force the NSX to reboot.

NetRanger-Specific Configuration

For information about configuring individual NSX machines, please refer to the following section, which describes the nrconfig utility.

Complete the NetRanger Configuration Instructions and Worksheets

The NetRanger configuration utility (**nrconfig**) performs the initial configuration of the NetRanger NSX, Director, and BorderGuard files. Use the following worksheets as a guide for gathering the information for nrconfig (such as IP addresses, passwords, and names of network components).

You may find it convenient to make copies of these worksheets when you are ready to configure your NetRanger software.

NetRanger Configuration Instructions and Worksheets

Version 1.2.2

The Director and NSX systems are configured with a utility called nrconfig. In addition to being run at installation, this utility can be run at any time to change an existing configuration. This section includes worksheets to help you gather the information (such as IP addresses, passwords, and names of network components) you need before you run nrconfig.

Before you run nrconfig, you must have completed the pkgadd (Solaris) or swinstall (HP-UX) installation for one or more of the following NetRanger components:

- **The NSX (WGCnsx)**
- **The Director (WGCdrctr, WGCcfgs)**
- **The optional Database/File Management (WGCsapd) software**

New NSX systems are shipped with the packages installed, so you only need to install the packages on NSX or Director systems that you are upgrading.

You must also have gathered the following information about your network:

- **IP Addresses of all network components**
- **Names of all network components**
- **Services you wish to allow in and out of your network (NSX Install)**
- **NetRanger Organization IDs and Names**
- **Routing Information (both IP and NetRanger)**
- **Passwords and other host information**

NOTE

You must run nrconfig as user netrangr. nrconfig can be run against an active NSX or Director system without having to shut down any of the NetRanger daemon services.

The NetRanger Configuration Program

nrconfig initially displays the following prompt:

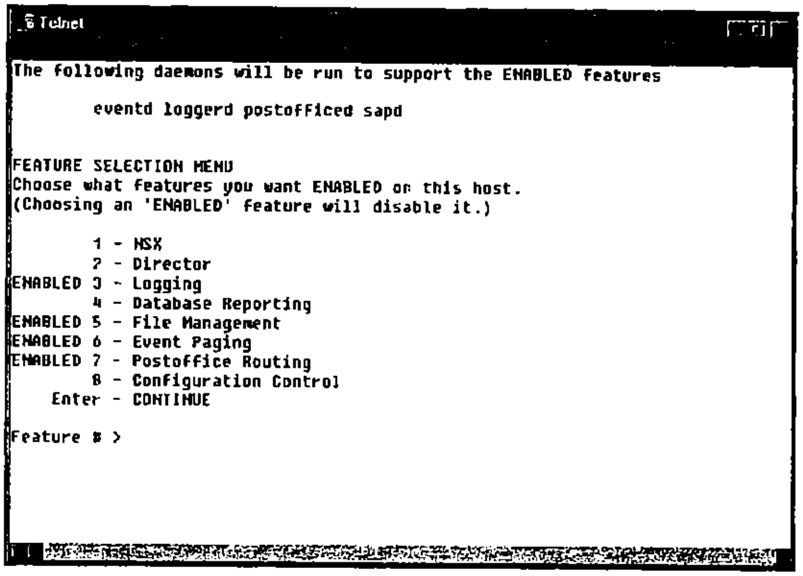
```
Are you ready to continue with configuration of your NetRanger? (y/n)>
```

If you have gathered the required information and are ready to configure the NetRanger software, choose `y` then press the **Enter** key to continue.

FEATURE SELECTION MENU

This menu, which is shown below, prompts you to select which features you want this installation to support.

When you select a feature from the menu, it is prefixed by "ENABLED" to indicate that it is presently selected. To disable a selected feature, simply choose it from the menu again. The list of daemons required to support the "ENABLED" features is shown at the top of the screen above the Feature Selection menu.

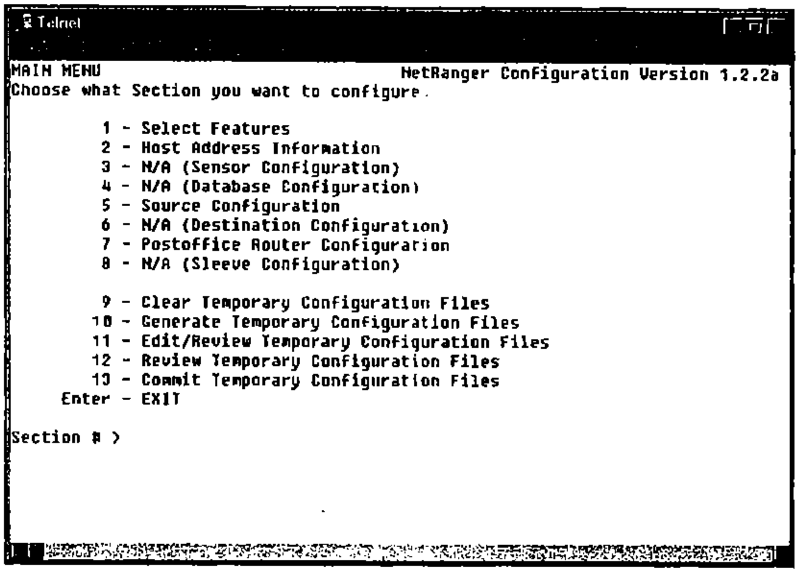


```
The following daemons will be run to support the ENABLED features

        eventd loggerd postofficed sapd


FEATURE SELECTION MENU
Choose what features you want ENABLED on this host.
(Choosing an 'ENABLED' feature will disable it.)

        1 - NSX
        2 - Director
ENABLED 3 - Logging
        4 - Database Reporting
ENABLED 5 - File Management
ENABLED 6 - Event Paging
ENABLED 7 - Postoffice Routing
        8 - Configuration Control
    Enter - CONTINUE

Feature # >
```

To continue with NetRanger Configuration, choose **Enter** at the menu prompt. This takes you to :he Main menu You can return to this or any other menu at any time from the Main menu.

MAIN MENU

Each menu item takes you through a series of subordinate, or "child", menus that are organized by feature requirements. Features that are not required for the specified NetRanger configuration are preceded by N/A (Not Available). For example, in the figure below, options 3, 4, 6, and 8 are not available because they are not required to support the configuration specified in the Feature Menu shown on the previous page. You can return to a configuration menu item at any time by selecting option 1 from the Main menu without losing any information that you may have already input.



```
MAIN MENU                                  NetRanger Configuration Version 1.2.2a
Choose what Section you want to configure.

          1 - Select Features
          2 - Host Address Information
          3 - N/A (Sensor Configuration)
          4 - N/A (Database Configuration)
          5 - Source Configuration
          6 - N/A (Destination Configuration)
          7 - Postoffice Router Configuration
          8 - N/A (Sleeve Configuration)

          9 - Clear Temporary Configuration Files
         10 - Generate Temporary Configuration Files
         11 - Edit/Review Temporary Configuration Files
         12 - Review Temporary Configuration Files
         13 - Commit Temporary Configuration Files
      Enter - EXIT

Section # >
```

The following pages contain worksheets to help you organize your nrconfig information. Each worksheet identifies the required features. You can skip those pages that discuss features that have not been 'ENABLED.'

1 - Select Features

This menu item takes you to the Feature Selection menu with which you were initially presented.

2 - Host Address Information

(Required for all Installations)

LOCAL HOST ADDRESS MENU

Enter this NetRanger's names and IDs in the following fields.

1 - **Organization Name** ____________________

2 - **Organization ID** ____________________

3 - **Host Name** ____________________

4 - **Host ID** ____________________

3 - Sensor Configuration

(Required for NSX)

BorderGuard CONFIGURATION MENU

Enter BorderGuard Configuration data into the following fields:

1 - **BorderGuard's Network Host Name** ____________________

2 - **BorderGuard's PASSWORD** ____________________

3 - **BorderGuard's Version ID/Mode** **V3, V4Router, V4Bridge**

BorderGuard's Network Host Name—This is the network host name for the BorderGuard used in /etc/hosts on the NSX or in DNS.

BorderGuard's PASSWORD—This is the password used to log into the BorderGuard.

BorderGuard's Version ID/Mode—This is the BorderGuard's Version ID and Configuration Mode. The BorderGuard Version 3 software only supports Router mode. The BorderGuard Version4 NetSentry software supports either Router or Bridge mode. The default is Version 4 Bridge Mode.

Based on the **BorderGuard's Version ID/Mode,** the following configuration menus refer either to *Router Mode or Bridge Mode Configuration.*

Router Mode Configuration

> NOTE
>
> The next menu is the first example of a configuration menu that allows a list of entries. You can add as many entries to the list as you can see on your screen. Each Entry menu allows you to Add, Edit, or Delete entries in the list.

This section establishes the IP addresses and netmasks for the BorderGuard's Network Interfaces (The BorderGuard network device should separate your protected networks from outside untrusted networks).BorderGuard LAN Interfaces Entry menu

Each entry contains the following two fields:

1 - Interface IP Address

2 - Interface Netmask

IP Address **NetMask**

________________ ________________

________________ ________________

________________ ________________

IP Address—This is the IP Address used by the BorderGuard on the subnet connected to this interface.

NetMask—This is the IP mask used on the subnet connected to this interface.

BorderGuard WAN Interfaces Entry menu

Each entry contains the following two fields:

1 - Interface IP Address

2 - PPP Destination IP Address

IP Address **PPP Dest IP Address**

________________ ________________

________________ ________________

________________ ________________

IP Address—This is the IP Address used by the BorderGuard for this PPP interface.

PPP Destination IP Address—This is the Destination IP Address used by the BorderGuard for this PPP interface.

BorderGuard ROUTER CONFIGURATION MENU

Enter BorderGuard Router Configuration data into the following fields:

1 - **BorderGuard's Primary IP Address** ____________________

2 - **BorderGuard's default gateway** ____________________

3 - **Minutes to log on an event** ____________________

4 - **Minutes to shun on an event** ____________________

5 - **NSX IP Address** ____________________

6 - **BorderGuard's IP Address connected to NSX** ____________________

7 - **BorderGuard's External IP Address** ____________________

BorderGuard's IP Address—The NetRanger system is this IP Address to establish encrypted sleeves and to communicate with the NSX.

NOTE
If you are using encrypted sleeves over the Internet, this should be a routeable Internet Address.

BorderGuard's default gateway—This is the IP Address that the BorderGuard should use for its default gateway for IP packet routing.

Minutes to log an event—This is the maximum number of minutes to log an event in an IP session.

Minutes to shun on an event—This is the maximum number of minutes to shun.

NSX IP Address—This is the IP Address used by the NSX on the subnet connecting the NSX to the BorderGuard.

BorderGuard's IP Address connected to NSX—This is the IP Address used by the BorderGuard on the subnet connecting the NSX to the BorderGuard.

BorderGuard's External IP Address—The NetRanger uses the External IP Address as the connection to the untrusted networks.

STATIC ROUTES ENTRY MENU

This section establishes the IP Addresses, Netmasks, and Gateway IP Addresses for the Static Routes to be implemented by the BorderGuard. Each entry contains the following three fields:

1 - Network's IP Address

2 - Network's Netmask

3 - Network's Gateway IP Address

Network's IP Address	**Network's Netmask**	**Network's Gateway IP Address**

Network's IP Address—This is the IP Address for the subnet for the static route.

Network's Netmask—This is the netmask for the subnet.

Network's Gateway IP Address—This is the IP Address that acts as a gateway to the subnet for the static route.

Bridge Mode Configuration

BorderGuard ROUTER CONFIGURATION MENU

Enter BorderGuard Router Configuration data into the following fields:

1 - BorderGuard's IP Address ______________________________

2 - BorderGuard's default gateway ______________________________

3 - Minutes to log an event ______________________________

4 - Minutes to shun an event ______________________________

5 - NSX IP Address ______________________________

BorderGuard's IP Address—The NetRanger system uses this IP Address to establish encrypted sleeves and to communicate with the NSX.

NOTE
If you are using encrypted sleeves over the Internet, this should be a routeable Internet Address.

BorderGuard's default gateway—This is the IP Address that the BorderGuard should use for its default gateway for IP packet routing.

Minutes to log an event—This is the maximum number of minutes to log an event in an IP session.

Minutes to shun on an event—This is the maximum number of minutes to shun.

NSX IP Address—This is the IP Address used by the NSX on the subnet connecting the NSX to the BorderGuard.

The following two sensor configuration menus refer both *Router Mode and Bridge Mode Configuration.*

SECURITY POLICY CONFIGURATION MENU

This section establishes which incoming services to allow on your interface, and includes the servers through which this traffic will be allowed to pass. Enter the Server IP addresses for the allowed services into the following fields:

1 - External FTP Access Server ____

2 - External TELNET Access Server____

3 - External MAIL Access Server____

4 - External WEB Access Server____

5 - External DNS Access Server ____

External FTP Access Server—This is the IP Address of the FTP Server that is allowed to service FTP requests coming in through the BorderGuard's External IP Address.

External TELNET Access Server—This is the IP Address of the TELNET Server that is allowed to service TELNET requests coming in through the BorderGuard's External IP Address.

External MAIL Access Server—This is the IP Address of the SMTP Server that is allowed to service SMTP requests coming in through the BorderGuard's External IP Address.

External WEB Access Server—This is the IP Address of the World Wide Web Server that is allowed to service HTTP requests coming in through the BorderGuard's External IP Address.

External DNS Access Server—This is the IP Address of the DNS Server that is allowed to service DNS requests coming in through the BorderGuard's External IP Address.

INTERNAL NETWORKS ENTRY MENU

This section establishes the IP Addresses and Netmasks for the Internal Protected Networks. Each entry contains the following two fields:

1 - Network's IP Address

2 - Network's Netmask

Network's IP Address **Network's Netmask**

________________________________ ________________________________

________________________________ ________________________________

________________________________ ________________________________

________________________________ ________________________________

________________________________ ________________________________

Network's IP Address—This is the IP Address for the subnet for the internal network.

Network's Netmask—This is the netmask for the subnet.

4 - Database Configuration

(Required for Database)

DATABASE CONFIGURATION MENU.

Enter the Database User ID and Password for NetRanger into the following fields:

1 - **Database USER ID**____

2 - **Database PASSWORD** ____

Database USER ID—This is the user id used to log into the database.

Database PASSWORD—This is the password used to log into the database.

5 - Source Configuration

(Required for Director/Logging/Database Reporting/Event Paging)

SOURCE ENTRY MENU

This section establishes the NetRanger's names and IDs and IP Routing Addresses for the sources of NetRanger Events. Each entry contains the following five fields:

1 - **Organization Name**

2 - **Organization ID**

3 - **Host Name**

4 - **Host ID**

5 - **IP Address to route through**

Org Name	**Org ID**	**Host Name**	**Host ID**	**via IP Address**

IP address to route through—This is the IP Address of the closest NetRanger Postoffice that can route NetRanger postoffice packets to the destination.

6 - Destination Configuration

(Required for NSX/Director)

DESTINATION ENTRY MENU

This section establishes the NetRanger's names and IDs, IP Routing Addresses, Destination Services, and Event Logging Levels for the destinations of NetRanger Events. Each entry has the following seven fields:

1 - **Organization Name**

2 - **Organization ID**

3 - **Host Name**

4 - **Host ID**

5 - **via IP Address**

6 - **Service**

7 - **Level**

Org Name	Org ID	Host Name	Host ID	via IP Address	Service	Level

IP Address to route through—This is the IP address of the closest NetRanger postoffice that can route NetRanger postoffice packets to the Source.

Service—This is the destination's NetRanger Service.

Level—This is the lowest level Alarm/Event that should be sent to the destination service.

7 - Postoffice Router Configuration

(Required for Postoffice Routing)

ROUTER ENTRY MENU

This section defines the NetRanger's names, Ids, and IP Routing Addresses for remote NetRanger nodes. Each entry has the following five fields:

1 - **Organization Name**

2 - **Organization ID**

3 - **Host Name**

4 - **Host ID**

5 - **IP address to route through**

Org Name	Org ID	Host Name	Host ID	via IP Address

IP Address to route through—This is the IP Address of the closest NetRanger postoffice that can route NetRanger postoffice packets to the Remote NetRanger node.

8 - Sleeve Configuration

(Optional for NSX)

SLEEVED NETWORK ENTRY MENU

This section establishes the Remote Organization ID, Remote IP Routing Addresses, and Remote Network Netmasks for Sleeved Networks. Each entry has the following three fields

1 - **Sleeve Remote Org ID**

2 - **Sleeve Remote IP Address**

3 - **Sleeve Remote Netmask**

Sleeve Remote Org ID	Sleeve Remote IP Address	Sleeve Remote Netmask

Sleeve Remote Org ID— his is the Organization ID for the remote end of the sleeve.

Sleeve Remote IP Address—This is the IP address for the remote end of the sleeve.

Sleeve Remote Netmask—This is the subnet netmask for the remote end of the sleeve.

9 - Clear Temporary Configuration Files

This menu item prompts you to insure that you want to clear the temporary configuration files for the NetRanger software.

```
Are you sure you want to CLEAR the Temporary Configuration files? (y/n)>
```

Answer yes to clear and reinitialize the temporary NetRanger configuration files in /usr/nr/etc/wgc and the temporary BorderGuard configuration files in /usr/nr/etc/nsc to their default values.

10 - Generate Temporary Configuration Files

This menu item prompts you to insure that you want to generate the temporary configuration files for the NetRanger software.

```
Are you sure you want to GENERATE the Temporary Configuration files? (y/n)>
```

Answer yes to write the temporary NetRanger configuration files to /usr/nr/etc/wgc and the temporary BorderGuard configuration files to /usr/nr/etc/nsc.

NOTE

You should review the temporary NetRanger configuration files located in the /usr/nr/etc/wgc directory and the BorderGuard configuration files located in the /usr/nr/etc/nsc directory after nrconfig has generated the temporary configuration data. The temporary NetRanger configuration files **must** be committed to /usr/nr/etc (/tmp for temporary BorderGuard configuration files) after review or after any manual changes. The BorderGuard files must then be loaded onto the NSG BorderGuard.

11 - Edit/Review Temporary Configuration Files

This menu item starts a vi edit on the temporary NetRanger configuration files in /usr/nr/etc/wgc and the temporary BorderGuard configuration files to /usr/nr/etc/nsc.

12 - Review Temporary Configuration Files

This menu item starts a "more" command on the temporary NetRanger configuration files in /usr/nr/etc/wgc and the temporary BorderGuard configuration files in /usr/nr/etc/nsc.

13 - Commit Temporary Configuration Files

This menu item prompts you to insure that you want to commit the temporary configuration files for the NetRanger software to the NetRanger Configuration File Directory.

```
Are you sure you want to COMMIT the Temporary Configuration files to the
NetRanger Configuration File Directory '/usr/nr/etc' and to the BorderGuard
Configuration File Directory '/tmp'? (y/n)>
```

Answer yes to write the configuration temporary NetRanger configuration files to the /usr/nr/etc directory.

NOTE

This overwrites working NetRanger configuration files.

Enter - EXIT

To exit the NetRanger Configuration program, simply hit "Enter" at the menu prompt. This menu item prompts you to insure that you are ready to exit the configuration program.

```
Are you sure you want to EXIT? (y/n)>
```

Answer yes to exit the configuration program.

NOTE

You can exit and restart the NetRanger Configuration program without losing any of the configuration information you have input.

NetRanger configuration is complete.

NOTE

The NetRanger processes **must** be restarted using /usr/nr/bin/nrhup before the committed NetRanger configuration file will take effect.

NSX Installations

The BorderGuard Configuration Files **must** be uploaded to the BorderGuard and any manual BorderGuard Configuration changes, such as **Bridge Mode**, **must** be done before the commited changes will take effect.

Refer to *Initial Bridge Mode Configuration* for details on completing a Bridge Mode configuration.

If you are using a BorderGuard 2000 with Version 4.0 of the NetSentry software, then you may not have enough file space on the BorderGuard boot diskette to load the new BorderGuard configuration files. After you make backup copies of the files on the diskette, then you may delete the *readme*, *firewall.def* and *firewall.set* files which are not needed for normal operation.

IV Operating NetRanger

Working With the Director and the NSX

The NetRanger Director is the Graphical User Interface (GUI) for the NetRanger system. The NetRanger Director (also called "the Director")

- provides a graphical, intuitive display of information pertaining to network security violations in real time;
- displays a hierarchical map of the remote NetRanger software and hardware (the Sensor processes and the NSX hardware, for example) that send security notifications to the Director;
- provides utilities for configuration of the remote NetRanger applications; and
- provides utilities to query the database of historical security events.

The Director uses popular network management platforms like HP OpenView to display network security information. As a result of this integration, network management personnel do not have to learn multiple-user interface applications and paradigms to perform different network management tasks.

When a process on a remote NSX machine detects a security violation, a notification (called an "event") is sent from the NSX machine to the Director machine. The Director ensures that the machine and application that generated the event are represented on the graphical map, and then, if the event's severity level exceeds a user-definable threshold, the Director creates an Alarm icon on the map. The color of the Alarm icon is based on the severity of the event. The Application and Machine icons also change color, so it is easy to determine at a glance which machine detected the problem. With a few mouse clicks, details about the Alarm (source and destination IP address, for example) can be displayed. Location functions can be used to locate Alarms with specific properties.

Once an Alarm is diagnosed and addressed, the user can delete the Alarm icon from the user interface. The Application and Machine icons then revert to their previous state.

Architecture

The NetRanger Director is not a single computer program, but is rather a *set* of applications and background processes that work with a network management platform. The diagram below illustrates the data flow between the processes in NetRanger.

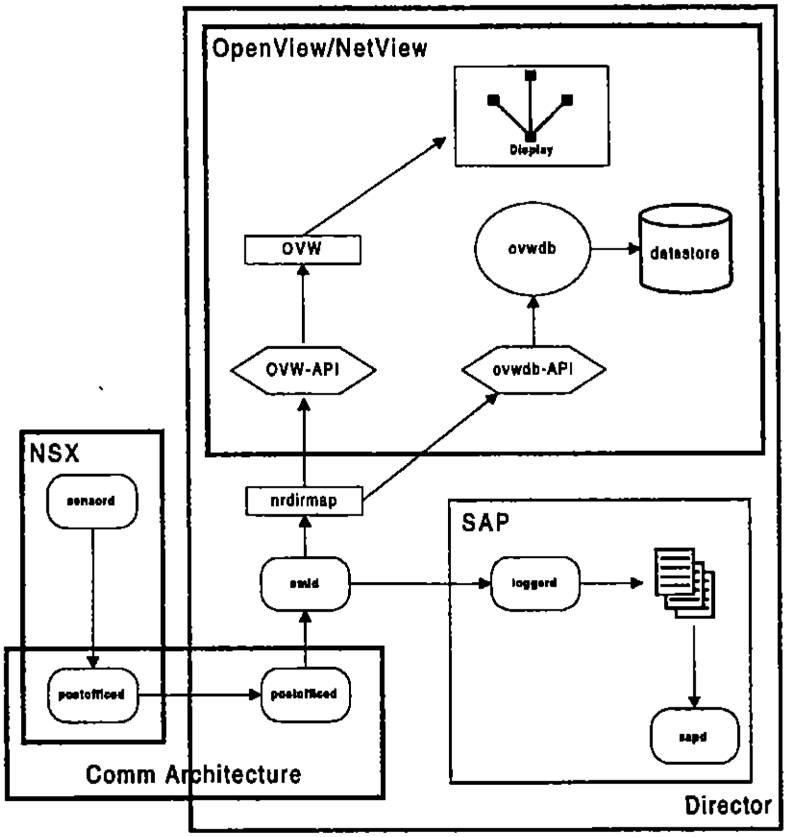


Figure IV-1: The NetRanger Director Architecture

In the diagram above, ovals represent background processes, squares represent foreground applications, cylinders represent datastores, hexagons represent APIs, and lines represent the flow of event data. Note that *ovw* and *ovwdb* are part of OpenView/NetView, *nrdirmap*, *smid*, and *loggerd* are part of the Director, and *sensord* is part of the NSX. Also note that the NSX and the Director both contain *postofficed* processes.

When the *sensord* process detects activity of interest, it generates an event that is sent via the *postofficed* daemons to the *smid* daemon on the Director machine. The *smid* daemon passes the event information to nrdirmap and the *loggerd* daemon, which logs the information.

nrdirmap looks at the severity level of the event. If the event severity exceeds a user-specified level, then *nrdirmap* tells *ovw* to draw an alarm icon. *nrdirmap* also tells *ovwdb* to create an alarm database object in the OpenView/NetView datastore.

Basic Director Functions

Starting the Director

The Director consists of three separate subsystems:

- The NetRanger background processes
- The network management platform background processes
- The network management platform user interface

> **NOTE**
>
> These subsystems should be started in the order listed above to ensure proper operation of the Director.

Starting the NetRanger Background Processes

The NetRanger background processes are configured to start automatically when the machine is rebooted, so in most cases, you will not need to manually start these processes.

In the event that you must start them manually, follow these steps:

1. **Log in as someone in the group** `netrangr`**, and then type**
   `nrstart`
2. **If the executable is not found, then type the fully qualified name,**
   `(/usr/nr/bin/nrstart)`

   put `/usr/nr/bin` **in your path,**

   or type
   `. /usr/nr/.profile.`

Starting the Network Management Background Processes

Like the NetRanger background processes, the network management platform background processes are configured to start automatically when the machine is rebooted, so in most cases, you will not need to manually start these processes.

In the event that you must start them manually, follow these steps:

1. **log in as** root **and then type:**

   ```
   ovstart
   ```

   If the executable is not found, then the subdirectory that includes the network management binaries is probably not in your path (the location for OpenView binaries is `$OV_BIN`**, and the location for NetView binaries is** `/usr/OV/bin`**). (To set your path, type** `. /usr/nr/.profile`**) Consult your network management documentation if you have difficulty starting the network management background processes.**

Starting the Network Management User Interface

To start the Director's network management user interface, follow these steps:

1. **If you use HP OpenView, log in as a user that belongs to the group** `netrangr` **and then type:**

   ```
   ovw &
   ```

> **NOTE**
>
> The *nrdirmap* program will start automatically when you bring up the network management user interface. You will never have to manually start *nrdirmap.*

Stopping the Director

To stop the Director, stop the subsystems in the *opposite* order in which they were started.

Stopping the Network Management User Interface

1. **If you use HP OpenView, select the menu option**

   ```
   Map..Exit
   ```

Usually, you will only want to close the user interface. In most circumstances, you will not want to close the background processes. If you do want to close the background process, follow the steps below.

1. **Log in as user** root **and then type**

   ```
   ovstop
   ```

   If the executable is not found, then the subdirectory that includes the network management binaries is probably not in your path (the location for OpenView binaries is `$OV_BIN`**, and the location for NetView binaries is** `/usr/OV/bin`**). Consult your network management documentation if you have difficulty starting the network management background processes.**

Stopping the NetRanger Background Processes

To stop the NetRanger background processes, follow these steps:

1. **Log in as someone in the group** `netrangr` **and then type**

   ```
   nrstop
   ```

2. **If the executable is not found, then either type the fully qualified name**

   ```
   (/usr/nr/bin/nrstop)
   ```

   or put `/usr/nr/bin` **in your path.**

Checking the Status of the Director Processes

To check the status of all Director processes, follow these steps:

1. **To ensure that the network management background processes are running correctly, type**

   ```
   ovstatus
   ```

2. **To ensure that the NetRanger background processes are running correctly, type**

   ```
   nrstatus
   ```

   If either of these executables cannot be found, check your path.

Understanding the Director's Submap Hierarchy:

When you double-click on a symbol, a submap is opened. This submap could have many symbols on it, and you can double-click these symbols to reveal more submaps. These descending submaps can be thought of as an upside-down tree with more and more branches. This upside-down tree structure is called the "submap hierarchy."

Traversing the submap hierarchy that nrdirmap creates is easy once you understand the following structure:

This type of submap...	can contain these symbols:
Root	Collection
Collection	Machines (NSX and Director)
	Collections
	Connections
Machine	Applications
Application	Alarms
	Alarm Sets

NOTE

Connections and Alarms do not have submaps. They represent the "leaves" in the submap tree.

Figure IV-2 illustrates the root submap. It is the highest level submap in the hierarchy. The root submap has no "parent submap". On the root submap, there should be a symbol representing a Collection of machines.

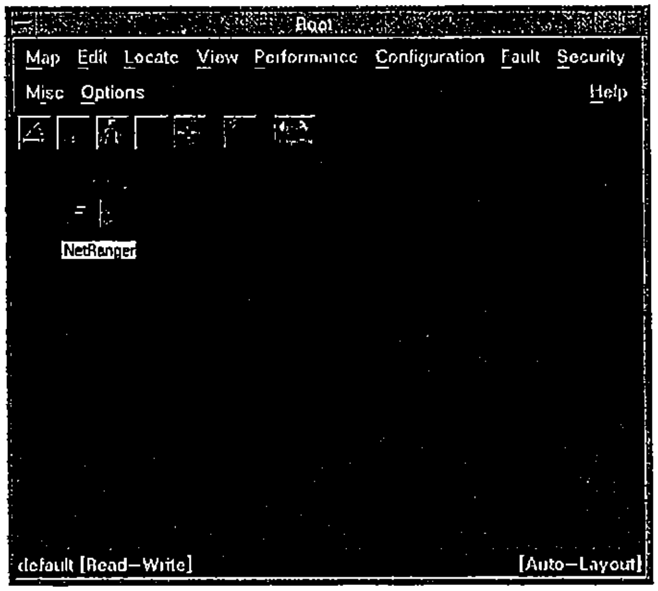


Figure IV-2: The NetRanger Director Submap

When you double-click on a Collection symbol like the one shown in Figure IV-2 , a Collection submap is displayed. A Collection submap can have NSX Machines, the Director Machine, other Collection symbols, and Connections between Machines. The Collection submap shown on the following page only contains a Director machine symbol.

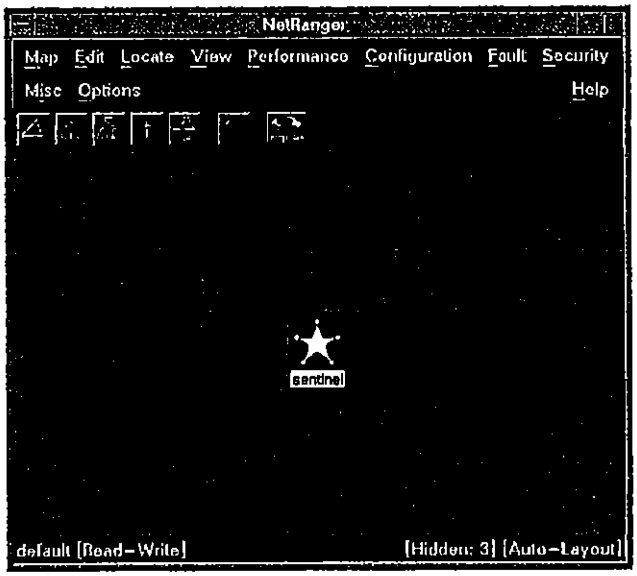

NetRanger
Map Edit Locate View Performance Configuration Fault Security
Misc Options Help
sentinel
default [Read–Write]
[Hidden: 3] [Auto–Layout]

Figure IV-3: A Collection Submap

When you double-click on a Machine symbol, a Machine submap is displayed. A Machine submap contains symbols that represent the different applications running on the machine. Refer to Chapter I for an overview of these application daemon services.

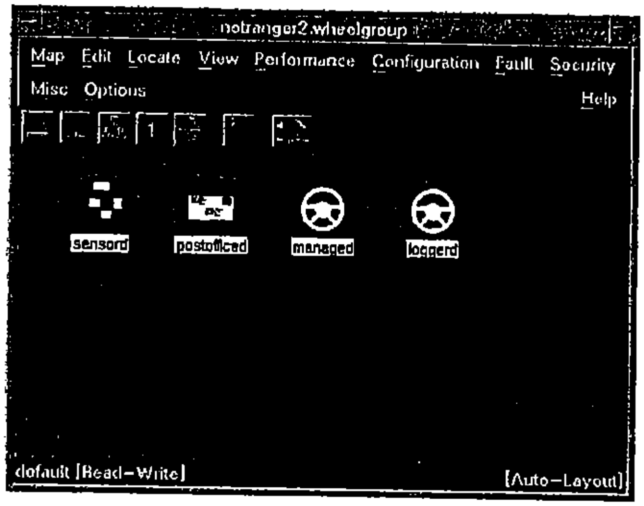


Figure IV-4: A Machine Submap

When you double-click on an Application symbol, an Application submap is displayed. An application submap contains alarms that that application had generated. For instance, if the *sensord* application for a machine generates an event and sends it to the Director, the Director will draw an alarm icon on the submap belonging to that machine's application.

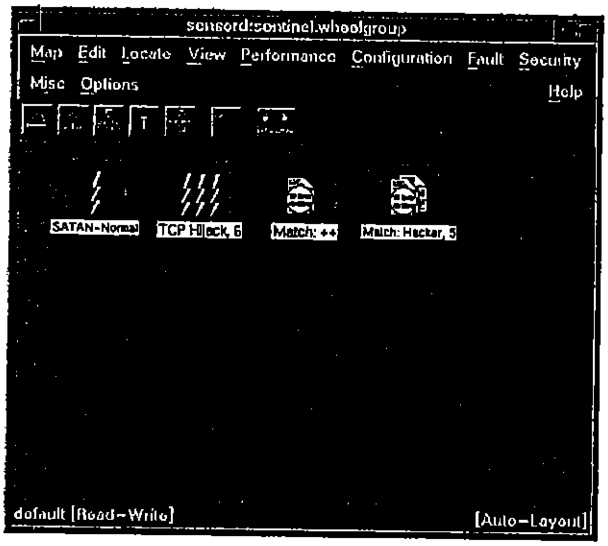


Figure IV-5: An Application Submap

For most alarms, the label under the alarm symbol will match the alarm's "Alarm Name" attribute. For instance, an alarm with the Alarm Name "Net Sweep" will have a "Net Sweep" symbol label.

Alarms with the name "String Match" and "Sec Violation" (Security Violation) will have their symbol labels taken from the "Alarm Details" attribute. This is because there are many types of Security Violations, and there are an infinite number of potential string matches, so for these two alarm types, the Alarm Name itself is not specific enough. For Security Violation alarms, the label will match the name of the specific violation, and for String Matches, the label will be the string that was detected.

Application submaps can also contain a special Alarm symbol called an "Alarm Set". An Alarm Set is created when multiple alarms are received that are identical in all respects *except for* timestamp *and* sequence number. For example, if you get 20 string match alarms with the same attributes (source and destination address, source and destination port, etc.), then the 20 alarms will be represented by a single Alarm Set symbol.

Alarm Sets can be differentiated from Alarms in two ways. First, the end of an Alarm Set symbol label will have a comma followed by the number of alarms represented by the Set. Second, the Alarm Set symbol type is slightly different from an Alarm symbol type. An Intrusion Alarm icon has one lightening bolt and an Intrusion Alarm Set has multiple lightening bolts. A String Match Alarm icon has one sheet of paper behind a magnifying glass and a String Match Alarm Set icon has multiple sheets of paper behind a magnifying glass.

If an Application has generated no Alarms, then a special Alarm called an "OkAlarm" will be displayed that indicates that the Application has no unresolved Alarms.

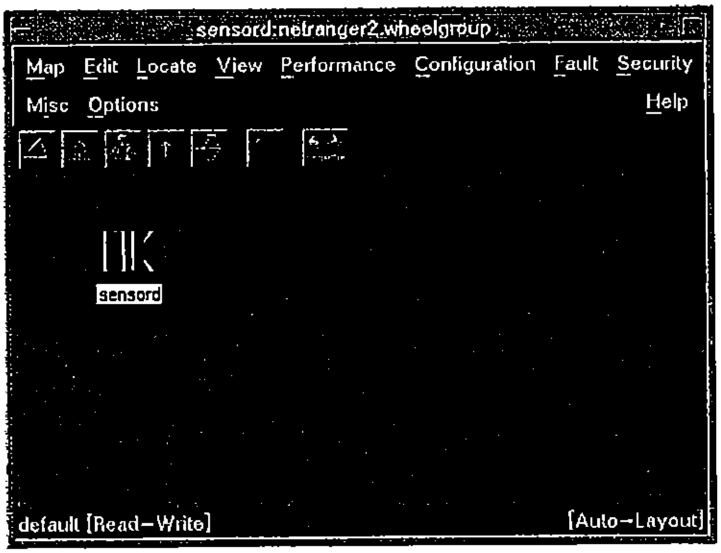

sensord:netranger2.wheelgroup
Map Edit Locate View Performance Configuration Fault Security
Misc Options
Help
OK
sensord
default [Read-Write]
[Auto-Layout]

Figure IV-6: An OkAlarm

Adding Entities

In general, there are four types of icon symbols: alarms (which include Alarm Sets and OK Alarms), applications, machines, and collections.

Alarm symbols, at the bottom of the submap hierarchy, can only be created by the *nrdirmap* application. An alarm symbol is created whenever an event that exceeds a user-defined threshold is received. There is no way for a user to manually create an alarm symbol.

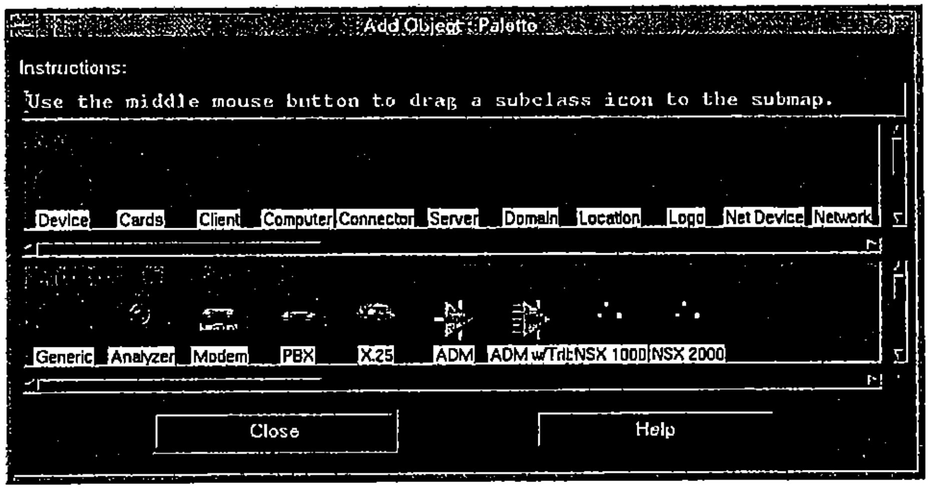
There are two ways that Application and Machine symbols can be created. First, if an application or host from which an event emanates is not already represented in the map, then *nrdirmap* will create the symbols for you.

If you do not want to wait until an alarm comes in to have a machine or an application represented in a map, you can add the symbols manually. The next two sections describe how to add machines and applications.

Manually Adding an NSX Machine Symbol

To manually add an NSX machine symbol, follow these steps:

1. **Double-click on a Collection symbol to open the Collection submap (the symbol on the root submap labeled "NetRanger" is a Collection symbol).** Machines can only be added to Collection submaps! **Do not try to add a Machine to a non-Collection submap.**
2. **Select the** Edit→Add Object **menu function. The** Add Object Palette **will appear.**
3. **Click on the** Net Device **icon. Several icons will appear in the bottom of the palette (see picture below).**



Add Object :Palette

Instructions:

Use the middle mouse button to drag a subclass icon to the submap.

Figure IV-7: The Add Object Palette

4. **Position the mouse pointer over the** NSX 2000 **icon, press and hold the** middle **mouse button, and drag the** NSX 2000 **icon to the collection submap. An** Add Object **window should appear.**
5. **Select** NetRanger/Director **from the list, and press the** Set Object Attributes **button.**
6. **In the** hostname **field, enter the name of the NSX machine exactly as you entered it in the /usr/nr/etc/hosts file.**
7. **Press the** Verify **button. If you entered the hostname correctly, NetRanger/Director will populate the Organization and Host Id fields for you.**
8. **Once the** hostname, Organization ID, **and** Host ID **are correct, press** OK.
9. **Press the** Set Selection Name **button. Choose the selection name from the list and then press** OK **in the Selection Name window. Press the** OK **button in the Add Object Window.**

Manually Adding an Application Symbol

1. **Double-click on the NSX Machine to which you wish to add the application.** Applications can only be added to Machine submaps! **Do not try to add an Application to a non-machine submap!**
2. **If the** Add Object : Palette **is not already displayed, bring it up by selecting the** Edit→Add Object **menu function.**
3. **From the** Add Object : Palette**, click on the** WGC Application **icon. Several icons should appear in the bottom of the window.**
4. **Using the same technique described above, drag the application icon to the NSX submap.**
5. **Select** NetRanger Director **from the list, and press the** Set Object Attributes **button.**
6. **All fields will be populated for you. Press** OK.
7. **Press the** Set Selection Name **button. Choose the selection name from the list and then press** OK **in the Selection Name window. Press the** OK **button in the Add Object Window. You should see the Application icon turn green, because a green** OkAlarm **will be created automatically in the submap of the Application you just added.**

Manually adding the Director Machine

Normally, you will not need to manually add the Director Machine. The Director Machine symbol is added for you automatically when nrdirmap comes up the first time. However, it is possible to manually delete the Director Machine, and you may want to manually add the Director Machine back to the map at a later time. Also, if you ever change the Organization ID or Host ID of the Director, then you must delete the Director Machine symbol and add it back with the correct IDs.

Please note that only one Director Machine can be represented at a time. In a future release, this restriction may be eased, but for this release, you can only have one Director icon on a map.

The procedure for adding a Director Machine symbol is almost identical to the procedure for adding an NSX Machine symbol. The only differences are as follows:

- From the Object Palette, instead of clicking on the "Net Device" symbol class, click on the "Computer" symbol class.
- Instead of dragging an NSX Machine symbol from the palette, drag the Director Machine icon.
- When you press the **Set Object Attributes** button, you shouldn't have to enter any data. Unless configuration files (like /usr/nr/etc/hosts) are missing or incorrect on your Director Machine, nrdirmap should be able to fill in this information for you.

Manually Adding an NSX Collection

The **Top-Level NSX Collection** (the entity that appears on the root submap labeled **NetRanger**) is created for you. This is the only Collection that can appear on the root submap. Do *not* try to create additional Collections on the root submap.

NSX Collections are used to customize, or "partition," the map. NSX Collections are good tools to use for grouping machines into logical units. See the section in this chapter entitled *How to Customize a Map* for more information about specific uses of NSX Collections.

Follow these steps to add an NSX Collection:

1. **Double-click on the NSX Collection's submap to which you want to add the new NSX Collection.** NSX Collections can only be added to NSX Collection submaps! **Do not try to add an NSX Collection to a non-NSX Collection submap!**
2. **If the** Add Object : Palette **is not already displayed, bring it up by selecting the** Edit→Add Object **menu function.**
3. **From the** Add Object : Palette, **click on the** Location **icon. Several icons will appear in the bottom of the window.**
4. **Using the same technique described above, drag the symbol containing the WheelGroup Logo to the NSX submap.**
5. **Select** NetRanger Director **from the list, and press the** Set Object Attributes **button.**
6. **In the** NSX Collection Name **field, enter the name of the NSX Collection you just moved to the submap. This name can be any unique string. For example, "New York," "Building 162," or "10.1.1 Machines" would be legitimate NSX Collection Names.**
7. **Press the** Verify **button.**
8. **Press** OK.
9. **Press the** Set Selection Name **button. Choose the selection name from the list and then press** OK **in the Selection Name window. Press the** OK **button in the Add Object Window.**

Modifying and Viewing Entity Attributes

Once an entity has been created (either by a user or by *nrdirmap*), it is often helpful to view a listing of the entity's attributes. Some attributes can be edited by the user (for instance, a machine's Point of Contact), and other attributes are read-only (for instance, an alarm's Date). OpenView/NetView provides a visual indication of which fields are changeable and which are not.

To display an entity's attributes, select the entity with the mouse pointer, and then select the menu function **Edit→Describe/Modify→Object**. You can also select the entity and type Ctrl+O and you can also put the mouse pointer over the icon, press the right mouse button, and select **Describe→Modify Object**. A pop-up window will appear. Select **NetRanger Director** from the list of applications, and then press the **Configure** button.

Different entities have different attributes, so each entity will be discussed separately.

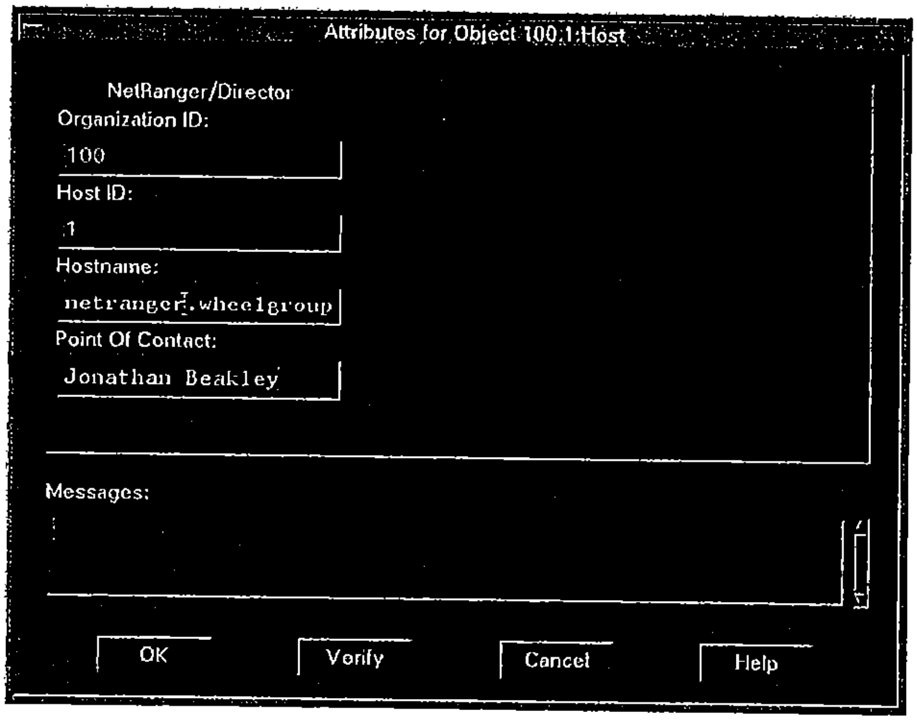
NSX Collection Attributes

The NSX Collection Name is the single attribute of a NSX Collection. If you change the Name, and then press **OK** on the appropriate screens, the NSX Collection's symbol label and submap name will change to reflect the new name.

Machine Attributes

Machines have four attributes: **Organization ID**, **Host ID**, **Hostname**, and **Point Of Contact**. The hostname and point of contact are editable, but the **Org ID** and **Host ID** are not. If you need to change an Org or Host ID, the best thing to do is to delete the machine and then re-add the machine with the correct IDs. If the hostname is changed, the Machine's symbol label will be the part of the hostname up to the first dot ("."), and the submap name will be the entire hostname.

If you want to store more information about the Point of Contact than the single field will contain, there are two things you can do. First, you can use the **Object Comments** field to store the additional point of contact information. Second, you could put the point of contact information in a separate trouble-ticketing system.



Attributes for Object 100;1:Host

NetRanger/Director

Organization ID: 100

Host ID: 1

Hostname: netranger.wheelgroup

Point Of Contact: Jonathan Beakley

Messages:

Figure IV-8: Object Attributes Window

Application Attributes

Machines have six attributes: **Application Name**, **Minimum Marginal Status Severity**, **Minimum Critical Status Severity**, **Alarm Consolidation Threshold**, **Organization ID**, **Host ID**, and **Application ID**. The application name, status severity fields, and consolidation threshold are editable, but the ID fields are not. If you need to change an ID, delete the application and then re-add it with the correct IDs. If the application name is changed, the Application's symbol label will change to match the new application name, and the Application's submap name will reflect the new name, too (the format for the Application submap name is **<hostname>:<application name>**).

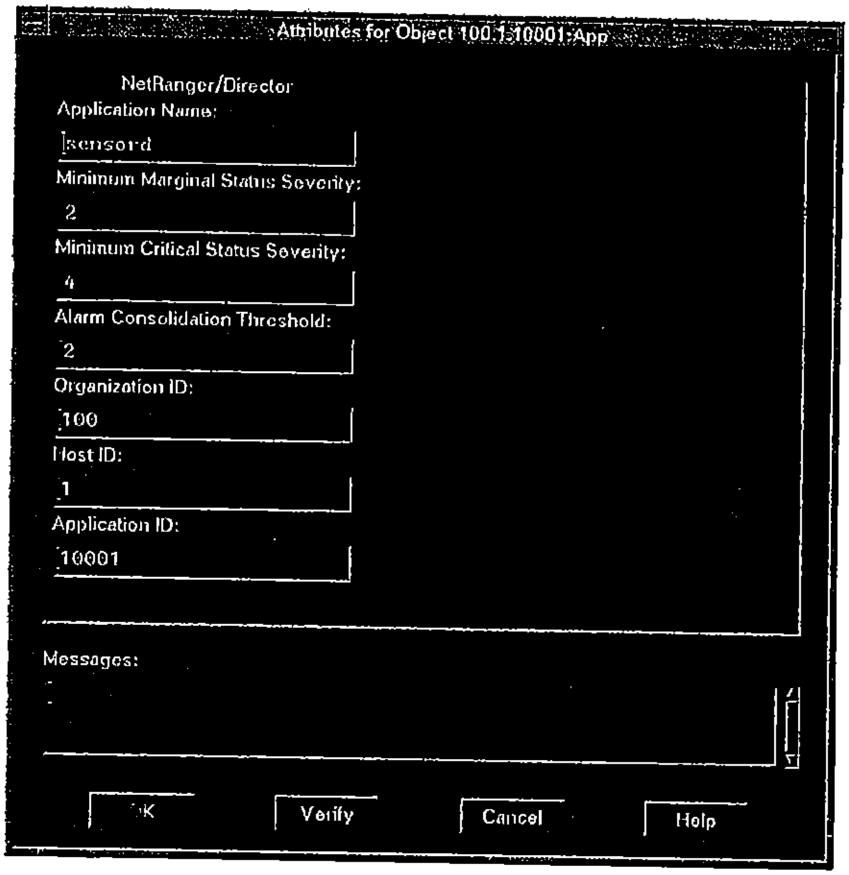
The **Minimum Marginal Status Severity** describes the lowest severity status an event can have before a marginal (yellow) alarm is created to represent that event. For example, if the minimum marginal status severity is 3, and a severity 2 alarm comes in, then no alarm entity will be created.

NOTE
The higher the severity level, the more severe the alarm. Currently, severity 5 is the highest severity level assigned by the *sensord* daemon.

The **Minimum Critical Status Severity** describes the lowest severity an event can have before a critical (red) alarm is created to represent that event. For example, if the minimum critical status severity is 3, and a severity 4 alarm comes in, then a critical alarm will be created.

NOTE
If you change a status severity value, only events generated **after the change** will be affected. If you increase a threshold severity level from 2 to 3, *nrdirmap* will not remove any existing level 2 alarms from the application's submap. Also, if you decrease a threshold severity level from 3 to 2, nrdirmap will not check historical log files and create alarm icons for severity level 2s that may have occurred in the past. Note that Connections and Alarms do not have submaps.

The **Alarm Consolidation Threshold** describes how many identical alarms must be received before the alarms are replaced by a single "Alarm Set" icon. By default, if two or more alarms are received that are alike in all respects except for timestamp and sequence number, nrdirmap will represent these alarms with a single "Alarm Set" icon. This prevents the screen from being cluttered when many similar alarms are received.



Attributes for Object 100:1:10001:App

NetRanger/Director

Application Name: sensord

Minimum Marginal Status Severity: 2

Minimum Critical Status Severity: 4

Alarm Consolidation Threshold: 2

Organization ID: 100

Host ID: 1

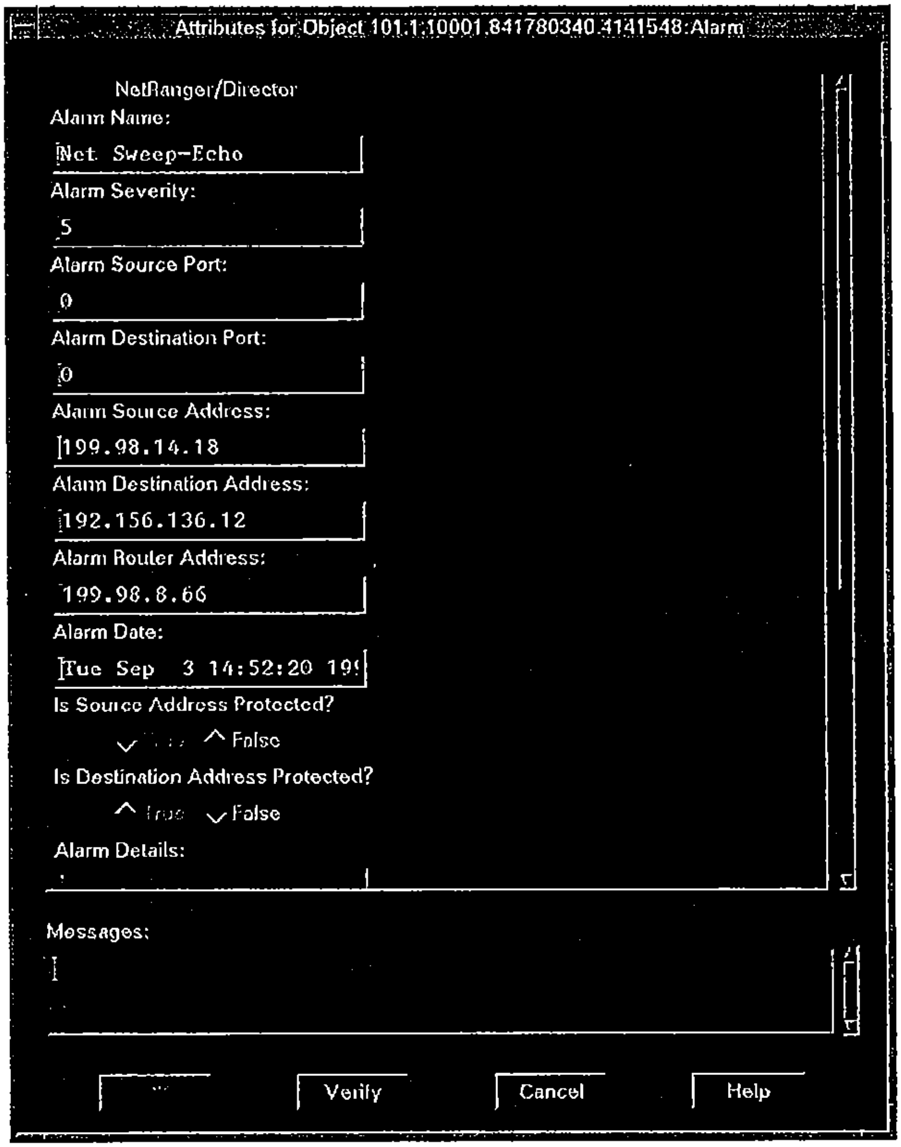
Application ID: 10001

Messages:

Figure IV-9: sensord Attribute Information

Alarm Attributes

Alarms have many attributes: **Name, Severity, Source Port, Destination Port, Source Address, Destination Address, Router Address, Date, Is Source Address Protected, Is Destination Address Protected, Details, Signature ID, Subsignature ID, Organization ID, Host ID, Application ID, Instance ID.** All alarm attributes are read-only.



Attributes for Object 101.1.10001.841780340.4141548:Alarm

NetRanger/Director

Alarm Name: Net Sweep-Echo

Alarm Severity: 5

Alarm Source Port: 0

Alarm Destination Port: 0

Alarm Source Address: 199.98.14.18

Alarm Destination Address: 192.156.136.12

Alarm Router Address: 199.98.8.66

Alarm Date: Tue Sep 3 14:52:20 19

Is Source Address Protected? [✓ True] False

Is Destination Address Protected? True [✓ False]

Alarm Details:

Messages:

Figure IV-10: Alarm Event Attributes

By default, when two or more alarms are received that are alike in all respects except for timestamp and sequence number, nrdirmap will represent these alarms with a single "Alarm Set" icon. The attributes of an Alarm Set are almost the same as the normal Alarm. The Alarm Set does not have a timestamp and sequence number. Instead, it has an Alarm Count, Date of First Alarm in Set, and Date of Last Alarm in Set.

Once an Alarm Set is created, if additional matching alarms are received, the Alarm Count is incremented, and the Alarm Date(s) are changed if applicable. Note that the symbol label for an Alarm Set is similar to an Alarm, except that after the Alarm Name, the Alarm Count is given.

The special **OkAlarm** that indicates that an application has no unresolved alarms has only four attributes: **Date, Organization ID, Host ID**, and **Application ID.** All these fields are read-only. The Date field specifies the time at which the **OkAlarm** was created. This gives a lower boundary to the last time that the application in question detected an attack.

Deleting Entities

When you want to remove a symbol (and its corresponding database object), you must select the symbol and then.choose the **Edit→Delete Object→From *All* Submaps** menu option. The most common usage of the delete function is deleting an alarm symbol once the potential hacking attempt has been diagnosed and resolved.

There are rules governing the deletion of symbols that help prevent the accidental removal of alarms and other symbols. One general rule to remember is this:

NOTE
Applications and Machines can NOT be deleted until ALL of their alarms have been deleted.

This forces the user to go into the submap containing the alarms and specify that it is OK to delete the alarms. This helps prevent a hacking attempt from going unnoticed.

Once an application or host has had all of its alarms resolved (and deleted),you are free to delete the application or machine.

NOTE
If you delete an application or machine, and then an event is received for that machine, the machine will be redrawn on the map. In a case like this, it might be better to *hide* the machine (see the description of the Hide function discussed later in this chapter).

Because it would be very easy to accidentally delete large groups of machines, non-empty Collections cannot be deleted. If you have a Collection that contains many machines, and you want to delete the Collection, you must first go into the Collection submap and delete all of the machines (and of course, the machines must have their alarms deleted before the machines can be deleted). Once you have emptied the collection submap, you can then delete the Collection.

NOTE

Never use the Delete Submap function! *nrdirmap* does *not* support this function. Always use the **Delete Object** function to delete entities!

How to Partition a Map

NSX Collection entities can be used to customize, or "partition" a map. If the number of NSX machines you are monitoring is too great to represent on a single submap (for instance, the Top-Level NSX Collection submap), you can create additional Collections, and then add Machine icons to those Collection submaps. This allows you to create a hierarchical grouping of machines.

For example, if you had 25 NSX machines in Los Angeles, and 35 machines in New York, you could create an "LA Collection" entity and a "NY NSX" Collection entity. You could then add the NY NSX Machines to the NY Collection, and then add the LA NSX Machines to the LA Collection. This allows you to have fewer symbols per submap, which makes locating symbols and diagnosing problems faster and easier.

NOTE

To put a machine in a collection, you must use the **Add Object** function. If a machine is already represented on the map, and you want to move the representation (the symbol) from one collection to another, you must delete the machine and then re-add it. ***nrdirmap* does *not* support the "Cut and Paste" functionality!** Use of the Cut and Paste functionality on *nrdirmap* entities will yield unexpected results. *You must delete a machine and then re-add it to move the machine symbol from one Collection to another.*

Changing Map Configuration Parameters

There are five global Map-level configuration parameters that can be set. To see these parameters select the menu option **Map→Maps→Describe/Modify**. You will then see a pop-up window. On this window, choose the **NetRanger Director** application, and then press the **Configure** button.

A window with five parameters will appear. You will see the following questions:

1. **Default lowest event severity that generates marginal icon?**
2. **Default lowest event severity that generates critical icon?**
3. **Default Number of Identical Alarms before Icon Consolidation?**
4. **Should nrdirmap be enabled for this map?**
5. **Should new security alarms be shown on the IP Map?**

The answer to the first question specifies the minimum severity an event must have before a marginal (yellow) Alarm is generated. For instance, if you set this value to 2, then if any new applications are created, these applications will have marginal alarms generated for events whose status is two and higher. Of course, if you manually reconfigure the Application symbol to have a new marginal status threshold, then this default value will be overridden.

The answer to the second question specifies the minimum severity an event must have before a critical (red) Alarm is generated. For instance, if you set this value to 3, then if any new applications are created, these applications will have critical alarms generated for events whose status is three and higher. Of course, if you manually reconfigure the Application symbol to have a new critical status threshold, then this default value will be overridden.

The answer to the third question specifies the number of similar alarms that must be received before the alarms are replaced with an "Alarm Set". For instance, if you set this value to 3, then if three identical alarms (identical in all respects except for sequence number and timestamp) are received, then these 3 alarm icons will be replaced with a single Alarm Set whose properties match those of the alarms that were replaced. This function limits screen clutter by reducing the number of icons on the screen.

The answer to the fourth question tells whether nrdirmap is enabled for the currently opened map. By default, all maps will have nrdirmap enabled. If nrdirmap is disabled for a map, then no NetRanger security information will be displayed on that map. This function can be used to control access to NetRanger information. Note: *This parameter can only be set when a map is created. Once a map is created, this parameter cannot be changed.* For more information on this option, see the section entitled Limiting Access to Security Information.

The fifth question asks if you want alarm icons to be drawn on the IPMap. *This option has no effect with this release. It may be used in a future version.* The IPMap is the submap hierarchy created by the ipmap application. The ipmap application is the part of OpenView/NetView that draws a picture of the IP Topology. The advantage of having alarms represented on the IPMap is that you can view Fault status and Security status on the same screen. The disadvantage is that performance is degraded because extra icons are being created.

NetRanger Director User Interface Menu Functions

On the main menu bar, the menu option called **Security** contains many useful NetRanger Director functions. These functions are described below.

Remotely Configuring NetRanger Daemons

There are two ways to change the configuration of NetRanger daemons running on remote NSX machines.

You can use the **nrget/nrset** infrastructure to modify daemon characteristics based on "tokens" that are specified by the user. These commands can be run from the command line of the Director machine.

You can also use the graphical browser utility that comes with the Director. To bring up the utility, select one or more Application or Machine symbols, and then select the menu option **Security→Configure**.

To learn more about nrConfigure, refer to the section in this chapter entitled *nrConfigure*.

Viewing Alarm Context Information

The **Security→Show→Context** menu function can be used to display data that was being transmitted across your network at the time a security event occurred. Context information is not available for all Alarm types. Currently, only Alarms that involve "string matching" contain context information.

The following signature IDs correspond to string matching alarms:

Signature ID	Type of string matching
3100-3104	e-mail
3200-3201	WWW
8000	General string matching

All Alarms that have the signature IDs shown above will be represented with "Alarm:Content" icons (icons containing a picture of a magnifying glass over a sheet of paper). These icons differentiate "Content" Alarms from "Intrusion" Alarms (which are represented by icons that contain pictures of lightning bolts).

To use the Show Context function, select one or more Alarm or Alarm Set icon(s), and choose **Security→Show→Context.** An "xnmappmon" window will appear that displays three fields:

- "String Matched"—this field displays the string that was matched. The maximum length of this field is 64 bytes.
- "Context Buffer 1"—this field displays up to 256 bytes of information that was transmitted in a single direction (either from or to the Server) at the time the string match occurred.
- "Context Buffer 2"—this field displays up to 256 bytes of information that was transmitted in the opposite direction (either to or from the Server) at the time the string match occurred.

NOTE

All non-printable ASCII characters are displayed using a "\" character and two hex digits. For example, <ctrl-g>, which has ASCII value "07" in hex, is represented as "\07". The ASCII character "\" itself is represented as "\\".

If there is no context information available for an Alarm, then the "xnmappmon" window will display the following message:

```
Could not find context alarm information for alarm <Alarm Name>.
```

Viewing Event Lists

To view an ASCII list of the latest events that have been generated for a given application or machine, simply select either an Application or a Machine symbol from the map, and then choose the menu option **Security→Show→Current Events.**

This will execute a program that parses the log files in /usr/nr/var, looking for *all* events for the entity selected. Please note that this will include events that may be below the threshold for creating alarms.

Also note that this window is dynamically updated as new events come in. This is why the "hourglass" mouse pointer never goes away. The program does not stop until you press the **Stop** button, because it is always looking for new events.

To stop the search for new events, press the **Stop** button. After you have done this, you can enter new IDs (org/host ID pairs, or org/host/app ID tuples) and restart the search with the **Restart** button. You can also use the various save and print utilities to store the data you have collected.

Press **Stop** and then **Close** to stop the event search and close the window.

The events are displayed with an OpenView/NetView utility called **xnmappmon** (X-node Manager Application Monitor). You can change the fonts and layout of this utility by changing the application defaults file for this utility (see your network management platform documentation for details).

Viewing Database Status and Configuration

The **Security→Show→DB Info** function can be used to show information about the status and configuration of the NetRanger logging and database staging infrastructure.

To use this function, click on a Machine icon that represents a machine running *sapd*, or click on a *sapd* Application icon, and then select **Security→Show→DB Info**. An xnmappmon window will appear with three headings.

Under the heading

```
        /usr/nr/var status for <orgId>.<hostId>.<appId>:
```

you will see information about the number and size of files in /usr/nr/var.

Under the heading

```
        Run-time history for <orgId>.<hostId>.<appId>:
```

you will see information about the number of database processes that have been run.

Under the heading

```
        Trigger configuration for <orgId>.<hostId>.<appId>:
```

you will see database configuration information in the format below.

In the following example, the ORACLE_LOAD trigger is configured such that the DBLoad process will run if the number of DIRFILES in /usr/nr/var/new is greater than or equal to 1.

```
  ORACLE_LOAD     DIRFILES        1       /usr/nr/var/new DBLoad
```

Resolving an Alarm's IP Addresses

The **Security→Show→Names** function can be used to find the hostnames of an alarm's source and destination IP addresses. To use this function, select one or more Alarm (or Alarm Set), and select **Security→Show→Names.**

An xnmappmon window will display the hostnames if they can be found. If the IP addresses cannot be resolved, you will see the following message:

```
      "*** <Resolver> can't find <IP Address>: Non-existent domain"
```

Determining the Version of a Remote NetRanger Daemon

The Director includes a utility called *nrVersion* that determines the Version of NetRanger code running on a machine. This function is helpful when diagnosing problems or upgrading software. To run nrVersion, simply select one or more Machine or Application symbol, and then choose **Security→Show→Version.**

An "xnmappmon" window will display the version numbers of all NetRanger applications that are selected, and/or the version numbers of all NetRanger applications on any machines that are selected.

If you see the following message

```
    Error: Problem sending query to nr.configd
```

then the version of nr.configd that you are using does not support this menu function. You should also ensure that nr.configd is running on the remote machine.

Shunning IP Addresses and Class C IP Networks

The **Security→Shun** functions can be used to manually shun (block) incoming IP traffic. To shun traffic that emanates from an Alarm's Source IP Address, select the Alarm (or Alarm Set), and choose **Security→Shun→Source IP**. To shun traffic that emanates from any IP address within the Class C Network that contains an Alarm's Source IP Address, select the Alarm (or Alarm Set), and select **Security→Shun→Source Net**.

In either case, an xnmappmon window will display the output of the nrexec command that was used to shun the traffic.

Please note that the default timeout value for the nrexec command is 10 seconds, and that the default duration for the shun is 1440 minutes (one day). To extend the duration, to stop the shunning, or to otherwise exercise more granular control, use the **Security→Configure** menu function.

Unshunning IP Addresses and Class C IP Networks

The **Security→Unshun** functions can be used to manually unshun (allow the transmission of) incoming IP traffic. These functions are used to "undo" the effects of the **Security→Shun** functions.

To unshun traffic that emanates from an Alarm's Source IP Address, select the Alarm (or Alarm Set), and choose **Security→Unshun→Source IP**. To unshun traffic that emanates from any IP address within the Class C Network that contains an Alarm's Source IP Address, select the Alarm (or Alarm Set), and select **Security→Unshun→Source Net**.

In either case, an xnmappmon window will display the output of the nrexec command that was used to unshun the traffic.

Please note that if traffic is not already shunned for the selected Alarm, then the Unshun action will have no effect.

Saving Object Data to a File

Use the **Security→Save To File** function to direct the attributes of one or more objects to a file. This is helpful if you want to send an e-mail message about alarm details to someone.

To use this function, select one or more symbols on the map, and then choose **Security→Save To File**. An ASCII file will be created in /usr/nr/tmp. The filename(s) will match the selection name(s) of the object(s) you selected.

This function uses the OpenView "ovobjprint" utility. For more information about ovobjprint, see the ovobjprint man page.

Finding Out About nrdirmap

Use the **Security→About** function to find information about the version of nrdirmap that you are using.

Changing IP Addresses, Hostnames, and NetRanger IDs

If you change the IP characteristics of either a Director or NSX machine, or if you change the NetRanger communication infrastructure characteristics (like hostId, orgId, host name, and organization name), you *must* ensure that the appropriate configuration files have been changed on *all* your NetRanger machines, including the Director machine.

If you change the hostId or organizationId of either an NSX machine or the Director machine, after making the necessary changes to the configuration files, ensure that you use the **Edit→Delete** menu option to delete the machine from the map. After this is done, use the **Edit→Add Object** menu function to add the machine back to the map with the proper Ids. See the sections on adding and deleting objects for more information about these procedures.

If this changes. . .	**ensure that it is changed here, too (use the nrconfig utility to make changes):**
an IP Address	/usr/nr/etc/routes, /usr/nr/etc/sensord.conf, and /usr/nr/etc/managed.conf
host or organization names	/usr/nr/etc/auths, /usr/nr/etc/destinations, /usr/nr/etc/hosts, /usr/nr/etc/routes, and /usr/nr/etc/smid.conf
host or organization Ids	/usr/nr/etc/hosts

If the IP address or hostname of the network management station must be changed, consult your network management documentation to learn about what configuration changes must be made to your network management platform. On HP systems, it is recommended that you shut down the user interface, stop the OpenView daemons, stop the NetRanger daemons, and then use sam to reconfigure the IP information. If you are changing the hostname, you should run `/etc/set_parms hostname` to ensure that the Common Desktop Environment is aware of the new hostname. Once this is done, and once any additional OpenView-specific configuration is complete (as specified in the OpenView documentation), it is recommended that you reboot your machine.

Changing Registration Files

All OVw Applications have a configuration file called a Registration File that tells the User Interface (OVw) how to treat the application. On HP systems, registration files are kept in `$OV_REGISTRATION/C`.

In general, registration files should not be modified, but there are a few circumstances in which it is helpful to edit registration files. Registration files contain the command that is actually used to launch the OVw Application, so registration files are good places to edit an OVw Application's command-line parameters.

The following table lists nrdirmap's command line parameters:

Opt	Params	Function
-a	<int>	default Alarm consolidation threshold for new maps
-c	<non-zero int>	default Critical value threshold for new maps
-d	<none>	Disable nrdirmap for new maps by default
-f	<none>	force Full synchronization
-m	<non-zero int>	default Marginal value threshold for new maps
-p	<none>	Propagate to IPMap for new maps
-s	<int>	number of Seconds to be idle before sleep
-t	<none>	Tracing enabled

-a, Alarm consolidation threshold

By default, if two or more alarms are received that are alike in all respects except for timestamp and sequence number, nrdirmap will represent these alarms with a single "Alarm Set" icon. This prevents the screen from being cluttered when many similar alarms are received.

An alarm consolidation threshold is configurable for each application object that is represented in the map.

The -a option is used to define a new *default* alarm consolidation threshold. This default value is applied to all application objects that are created *after you change the default value.* For example, if all of the application icons in your map have an alarm consolidation of 2, and then you set the -a option to 5, then whenever a new application is created, the new application will have the threshold of 5. Please note that the -a option will have no effect on *existing* application entities.

The default is 2. A value of 0 means no alarm consolidation. Any integer zero or higher is valid.

-c, Critical value threshold

By default, if nrdirmap receives an event with a severity level of 4 or higher, the symbol that represents that alarm will have "Critical" status. Unless the user specifies otherwise, a symbol with Critical status will be red.

A critical value threshold is configurable for each application object that is represented in the map.

The -c option is used to define a new *default* critical value threshold. This default value is applied to all application objects that are created *after you change the default value*. For example, if all of the application icons in your map have a critical threshold of 4, and then you set the -c option to 3, then whenever a new application is created, the new application will have the threshold of 3. Please note that the -c option will have no effect on *existing* application entities.

-d, Disable nrdirmap by default for new maps

By default, when a new map is created, nrdirmap will be enabled, which means that nrdirmap will display security information on the new map. If you would like for nrdirmap to be disabled for new maps by default, add the "-d" option to the nrdirmap registration file.

See the section in this chapter entitled *Limiting Access to Security Information* for more information about enabling and disabling nrdirmap.

-f, force Full synchronization

By default, when a symbol that exists in multiple maps is deleted from a map, the symbol will not be redrawn on the map when the user interface is stopped and restarted. The idea is that once you delete a symbol from a map, the symbol is deleted permanently. Once a symbol is deleted from *all* maps, the object that the symbol represents is deleted from the object database.

This means that there could be objects in the database that might not be represented as symbols in one or more of your maps (for instance, if you have two maps, and you delete an alarm symbol from one of the maps, the alarm object is still in the database, but there is no symbol for that object in one your maps).

If you ever want to "refresh" a map to ensure that all objects in the database are represented in a map, use the -f option. This will force nrdirmap to represent all objects in the database as symbols on the map you just brought up.

Note that this option should have no effect if you only have one map.

If you have multiple maps, and you want to "recover" a symbol that was accidentally deleted from a map, you can use this option (assuming that the object is still represented as a symbol in another map).

-i, seconds to be Idle before sleep

By default, if nrdirmap does not receive an alarm or a user interface callback for 5 seconds, it will go to "sleep", and wake up once per second to check for new events. Once a new event is received, it will handle new events as fast as they come in, until 5 seconds pass with no more events. At this point, nrdirmap goes back to sleep.

-m, Marginal value threshold

By default, if nrdirmap receives an event with a severity level greater than or equal to 3 and less than the critical threshold value (discussed above), the symbol that represents that alarm will have "Marginal" status. Unless the user specifies otherwise, a symbol with Marginal status will be yellow.

A marginal value threshold is configurable for each application object that is represented in the map.

The -m option is used to define a new *default* marginal value threshold. This default value is applied to all application objects that are created *after you change the default value*. For example, if all of the application icons in your map have a critical threshold of 3, and then you set the -m option to 2, then whenever a new application is created, the new application will have the threshold of 2. Please note that the -m option will have no effect on *existing* application entities.

-p, Propagate to IP Map

This option currently has no effect. This option may be used in a later version of the product.

To change the amount of time in seconds before sleep, use this option. Under normal circumstances, there will be no reason to change this value from the default of 5 seconds.

-s, Secure map creation

Use this option to ensure that only authorized users can create maps that contain NetRanger information. When the "-s" option is enabled, maps with nrdirmap enabled can only be created from maps that already have nrdirmap enabled. This ensures that a user who does not have access to nrdirmap-enabled maps (and therefore, does not have access to security information) will not be able to create a map that has nrdirmap enabled.

See the section in this chapter entitled *Limiting Access to Security Information* for more information about enabling and disabling nrdirmap.

NOTE

Enabling the "-s" option will preclude creating nrdirmap-enabled maps from the command line using the `ovw -m <map name>` command. Once the "-s" option is enabled, the only way to create a new map with nrdirmap enabled is to open a map that already has nrdirmap enabled, and then use the **Map→Maps→New** menu function.

-t, Tracing enabled

If nrdirmap is malfunctioning, your authorized service representative might instruct you to enable tracing by adding the -t option. After you set this option, it is best to bring down the user interface, and then bring it back up by typing:

```
ovw > /usr/nr/tmp/nrdirmap.out
```

NOTE

This will create a file called nrdirmap.out with information that can be used by a WheelGroup representative to diagnose the problem. Please note that if you do not redirect the trace messages, the messages will go to standard out.

Command-Line Parameter Examples:

1. **To enable tracing, type**

   ```
   Command -Shared -Initial -Restart "nrdirmap -t";
   ```

2. **To create marginal icons for level 2 alarms and critical icons for level 3 and higher alarms, type**

   ```
   Command -Shared -Initial -Restart "nrdirmap -m 2 -c 3";
   ```

3. **To enable tracing and to create Alarm Sets once 15 similar alarms are received, type**

   ```
   Command -Shared -Initial -Restart "nrdirmap -t -a 15";
   ```

Changing the Number of Events Displayed in Event List

When you select a Machine or Application symbol and select the menu option **Security→Show Current Events**, by default the last 100 events associated with that entity are displayed (if less than 100 events are known, then all of the events are displayed). To change the number of events that are displayed, use an editor to modify the nrdirmap file, which is stored in `$OV_REGISTRATION/C` on HP systems.

Replace the "100" with the number of your choice on the line shown in bold.

```
        Action show_events  {
                SelectionRule (isWheelGroup && (isMachine ||
        isApplication));
                MinSelected  1;
                Command "sh -c 'unset OVwSessionLoc \;
                        $OV_BIN/xnmappmon \
                        -selectList \" ${OVwSelections} \" \
                        -commandTitle \" Show Current Events for \"
        \
                        -appendSelectList \
                        -appendSelectListToTitle \
                        -multipleDialogs \
                        -headingLine 2 \
                        -geometry 900x600 \
                        -followOutput \
                        -unbufIO \
                        -stopSignal 9 \
                        -cmd /usr/nr/bin/filterLogByHostApp -l 100' ";
            }
```

Changing Symbol, Object, and Submap Characteristics

The OpenView user interface (ovw) provides functions that modify characteristics of symbols (icons) and database objects.

Unfortunately, the user interface is perhaps a bit *too* powerful, in that it allows a user to change data in ways that can confuse the nrdirmap application. This section describes what user modifications are allowed and which are not.

Object Modifications

Object Modifications are made through the **Modify→Describe Object** menu function.

It is OK to change the "Comments" field, and it is OK to change any attribute field that is editable from the window that is accessed by selecting "NetRanger Director" and pressing the **View/Modify Object Attributes** button. Please note that any changes you make to an object *will apply to all maps.* Remember that symbols are map-specific, but database objects are shared among all maps.

You should not edit the Selection Name. The Selection Name field is a field that is used to uniquely identify an object.

Symbol Modifications

Symbol modifications are made through the **Modify→Describe Symbol** menu function.

You can change the "Display Label" setting, and you can change a symbol from "explodable" to "executable".

In general, changing the symbol label itself is not recommended, because nrdirmap has specific algorithms it uses to determine the symbol label, and it will override your label customization when the user interface is stopped and started.

You should not change the "symbol status source" because nrdirmap expects all symbols (except alarm symbols) to have "Compound Status Source". This ensures that an alarm's status is always propagated "upward" in the submap hierarchy. Changing the status source will jeopardize this.

You should not change the symbol type. This will cause "capability fields" in the object database to be changed, and this will affect many different functions—including synchronization and callback communication between nrdirmap and ovw. Do not change a symbol's symbol type.

Submap Modifications

Submap modifications are made through the **Modify→Describe Submap** menu function.

You can change the "Comments" and the "Background Graphics" fields.

Changing the "Submap Name" is not recommended because, like the symbol label, the submap name is set by nrdirmap, and nrdirmap will override your customization when the user interface is shut down and brought back up.

Searching for Symbols

OpenView provides fairly powerful search utilities. These search utilities can be used to locate symbols that match certain criteria. The following three search functions might be useful when searching for alarm symbols:

- Locate by Object Attribute
- Locate by Symbol Type
- Locate by Symbol Status

To use the Locate function, choose **Locate→Objects** from the main menu, and then pick the type of search you want.